Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 3 (2023)

Anonymity Maintenance Algorithm (Ama) Of Health Care Data from IoT Devices Using Edge System with Transfer Learning

A. Anitha
Research Scholar, Dept of Computer Applications, Dr. MGR Educational & Research Institute, Chennai, Tamil Nadu, India. anitha.amca@gmail.com

Dr. K. Selvam
Professor
Dept of Computer Applications, Dr. MGR Educational & Research Institute, Chennai, Tamil Nadu, India.
selwam2000@gmail.com

Abstract

In order to fully leverage the potential of the Internet of Things (IoT), it is crucial to safeguard against potential threats and prioritize the security and privacy of data collected and extracted from IoT devices. However, the implementation of security and privacy technology within IoT presents a number of unique challenges. This is due to the fact that IoT solutions comprise a diverse array of security and privacy solutions that are designed to safeguard IoT data at the device, infrastructure/platform, and application layers. As a result, ensuring end-to-end privacy protection across these three layers is a significant challenge within IoT. IoT devices implemented with recent advancements utilize edge system and monitors fitness of a person privately. In our proposed concept anonymity maintenance done along with privacy preserving in query processing in accordance with health monitoring values. In this edge system transfer learning applied to transfer minimum data which is privacy preserved to equip edge system about IoT devices in spite of their location. De-duplication will be done in edge system in health values monitoring thus frequency learning will be inculcated to know the frequency of that device in specified location. In health-oriented processing of query the privileges will be granted for each category of people to access integrity of data according to their standard of authentication. While granting privileges concerned person can handle all their available personal data using their authentic login details. Best edge system will be chosen using PSO or GWO techniques thus de-duplication implemented efficiently.

Keywords: Anonymity maintenance, query processing, de-duplication, Edge system, Categorization, Transfer learning, Frequency learning, Particle Swarm Optimization (PSO), Grey Wolf Optimization (GWO).

1. INTRODUCTION

The Internet of Things (IoT), which is the latest advancement of the internet, comprises of millions of devices that are utilized by different organizations and individuals for their specific purposes. The use of data from these IoT devices (also known as IoT objects) offers a unique opportunity to tackle problems that were previously too intricate and massive to be resolved. However, like any other web-based information, IoT data is exposed to various cyber security and privacy threats that can hold critical business or even national information hostage. In order to leverage the full potential of IoT, it is imperative to ensure the security and privacy of data collected and extracted from IoT devices by safeguarding against such threats.

Nonetheless, IoT presents numerous challenges that make it challenging to implement security and privacy measures. This is primarily because IoT solutions comprise of various security and privacy solutions that need to protect IoT data transported and stored across three different layers, namely the device layer, infrastructure/platform layer, and application layer. Thus, ensuring end-to-end privacy across these three layers is a significant challenge in IoT. In IoT privacy

protection and introduce new ideas for safeguarding IoT data privacy that can be used to ensure that IoT data remains private.

The privacy protection measures a multi-store IoT cloud that stores privacy information collected by the IoT. In IoT privacy protection that proposes novel strategies to acclaim privacy-preserving IoT architecture, maintain gender neutrality of IoT data, and protect IoT data privacy using a proof-of-concept approach that leverages multi-store IoT cloud and privacy storage protocol. IoT Architecture Protection Certificate and Concept Implementation introduce Certificate as extensions to support these strategies.

Since the start of the 21st century, the world has experienced significant growth in the field of information technology. This has led to a massive increase in the amount of data generated as businesses transitioned to digital platforms. Both humans and machines now produce vast amounts of data every day, making big data a reality. The potential benefits of big data are so significant in the rapid advancement of technology has also led to the creation of numerous industries, including tele-communications, healthcare, banking, and e-commerce.

The healthcare industry in particular has seen significant advancements in recent years, with the development of various tools and solutions such as sensors for detecting body temperature, blood pressure and heart rate. These solutions have generated 4,444 health records, each revealing new opportunities for extracting insights and key data. However, these tools and solutions also present unique challenges.

One of the most significant changes in healthcare innovation has been the increased use of electronic health records which are digital repositories of health and patient medical information from IoT devices. Monitored values are created using various methods to store electronic information in a single format, and they store information such as vital signs, allergies, weight, sex, medications, and patient x-rays. Medical centers and physicians use these values to support decision-making processes and inform patients about their treatment without letting out personal information. Despite the many advantages of using electronic solutions to store and transmit medical information, monitored values also come with numerous limitations and problems.

The main constituents of these systems are tags, text tags and media, which enable the provision of information about not only the presence of individuals, but also their contact details and addresses. The device count is usually ascertained using probability estimation methods, although the sensitivity of the system is restricted by environmental factors, such as humidity, and additional equipment. The subsequent phase is based on Wi-Fi access points, whereby devices such as laptops, smart watches and smart phones use frame searches to gauge the number of individuals present within a given area connected to the same access point. This approach leverages pre-existing systems and safeguards user privacy, while the main disadvantage is that it tends to overestimate the headcount of individuals with a higher number of devices and neglects those individuals who are not connected to the network. These systems have minimal infrastructure requirements and must comply with privacy laws. Nonetheless, most of these technologies are restricted to indoor spaces, and only a few can accurately count individuals, even in ideal conditions.

This manuscript is organized as follows. The introduction for the privacy protection measures of edge transfer learning. In next section the related existing works done and their reviews. The Anonymity maintenance Algorithm implementation will be explained in this section. The next section represents edge system for transfer learning methodology. The experimental results showing results of images tested. Finally, it presents conclusion for the anonymity maintenance.

I. RELATED WORK

The concept of Elite Opposition based learning and a chaotic k-best gravitational search (EOCS) methodology has been implemented at Yaun et al. The main key is to improvise the global exploring capabilities and rate of convergence with accuracy. In accordance with reliability and accurate predictions for EOCS based on technique known as grey wolf optimizer (GWO) is combined known as EOCSGWO algorithm that competes hardly.

In other existing system Zhao et al. it explains how the artificial humming bird algorithm (AHA) brought solutions to all optimization problems such as bio inspired optimization algorithm techniques. The comparison of AHA algorithm with humming birds attributes such as uniqueness in flight abilities and forage approaches in eco system.

The findings of AHA's validation are compared to those of several methods using two sets of quantitative test functions. The results demonstrate that AHA outperforms other meta-heuristic methods in determining high-quality alternatives

while requiring fewer control parameters. It discusses the importance of the swarm intelligence technique. This research presents a novel method to distribute workloads in a cloud-based environment. A load-balancing mechanism should take the convergence time into account. Even though fast convergence can quickly relieve overburdened VMs, Cloud Services' can promptly recover their performance and unexpected outcomes can be avoided.

I. IMPLEMENTATION OF ANONYMITY MAINTENANCE ALGORITHM (AMA)

In IoT devices such as mobile phones, iPads, and laptops, it is crucial to preserve the privacy of sensitive data during backup operations. This is especially important in devices like smart watches that monitor health and are constantly connected to the cloud to transmit health monitoring data to insurance companies that are in turn connected to local hospitals for immediate action. Emergency alerts will be sent to local hospitals by quickly querying the availability of doctors, specialists, beds, ambulances, or service care. The hospital is then quickly decided upon, and the admission process is triggered without revealing the patient's personal identity. All queries will be conducted only using health conditions and hospital details through an edge system database that contains available local data.

The edge system strictly adheres to privacy preservation by not leaking any personalized data, such as access through OTP or masked ID numbers showing only the last four digits. Unnecessary or redundant data is eradicated, such as in health monitoring where normal health conditions occurring over time do not need to be stored for extended periods. Instead of monitoring each device, categorization is done for each group based on their disease history, consistent monitoring of health and fitness, etc., and unwanted data is eliminated by setting threshold values for categorization. The edge system stores and tracks IoT cloud storage with respect to its location using transfer learning and implements transfer learning in different locations by transferring minimal data to other local edge systems where specified IoT devices are present. This data is saved for a period of time based on the frequency of the devices available in that location.

Frequency learning is implemented in transferring data to know the frequency of device availability in a locality. In health-oriented query processing, privileges are granted to each category of people to access data integrity according to their authentication standards. When granting privileges, the concerned person can handle all their personal data using their authenticated login details, while doctors or privacy keepers can access their data with an OTP only in the absence or during the serious condition of an authorized person. In the event of the above situation, this information will be shared with government officials as an emergency infringement. The best edge system will be chosen using PSO or GWO techniques, and efficient de-duplication will be implemented.

An integrated GWO-PSO algorithm utilizes the strengths of both techniques for achieving fast convergence and global optimization in selecting best edge system. These technologies enhance efficiency and resource allocation while effectively addressing parallel problems. In comparison to other conventional methods, the results of this study demonstrate significant potential, as global optimization facilitates quick integration and significantly reduces response times.

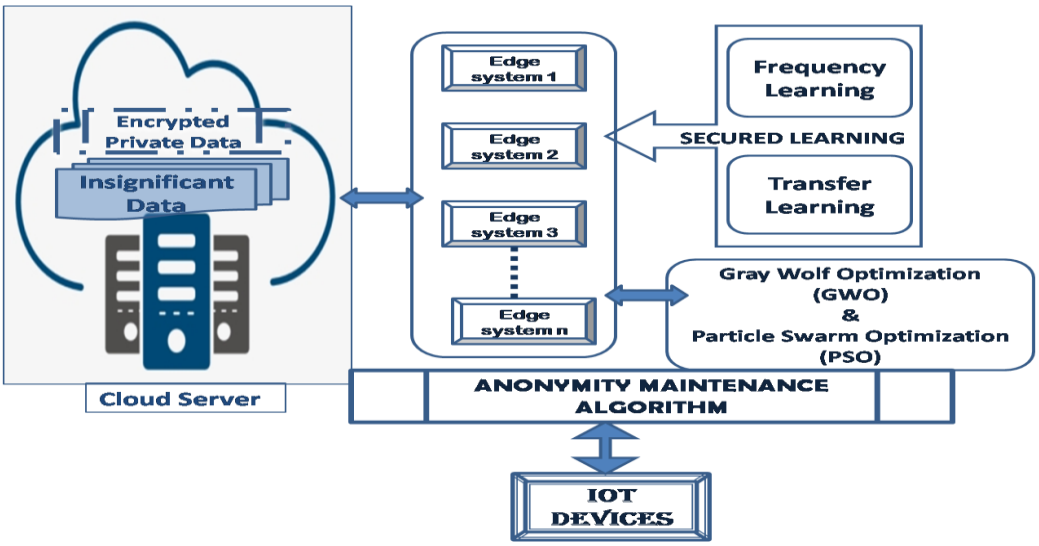

Figure.1 Anonymity Maintenance Algorithm Architecture

This algorithm has shown an average reduction of 12 percent in total response time, as compared to other algorithms. Moreover, the proposed GWO-PSO algorithm has obtained the best value for the objective function, increasing the PSO to 97.

Deep learning has garnered significant attention from researchers and achieved success in various domains. However, in certain fields like bioinformatics and robotics, generating large-scale data and providing comprehensive explanations can be challenging due to the high cost associated with data collection and annotation. This limitation hampers the progress of deep learning in these areas. To address the problem of inadequate training data, transfer learning has emerged as a promising approach, leveraging independent and distributed training and test data. This review aims to examine the current state of research on adaptive learning utilizing deep neural networks and their applications.

It begins by defining deep learning and categorizing recent research projects based on the techniques employed in deep learning. Machine learning algorithms have made significant contributions to computer science in recent years. However, the performance of these algorithms is often contingent upon the quality of representations derived from the training data. The learned representations should possess attributes such as clarity, discreteness, meaningfulness, and applicability to diverse tasks. Consequently, recent efforts have focused on developing deep learning models that excel at capturing high-resolution, nonlinear, and multidimensional images.

In this methodology it delves into the principles and advancements made in the process of representative learning and explore their application potential. Moreover, we conduct a comprehensive analysis of key issues, open challenges, and strengths associated with each framework or model under consideration.

The proposed system can provide accurate and comprehensive results by leveraging diverse data streams. However, transferring this extensive information can pose systemic challenges, and depending on the implementation, algorithm, and features, the model size can become large. Especially when dealing with distributed data files, the network can experience significant bottlenecks. An alternative approach to transfer learning is to employ distributed learning algorithms at each cloud edge and operate them independently of other edges, using local data isolated from the main server. However, not all edge nodes may require learning about the general information of the model. When environmental changes or operating patterns necessitate model replacement, it can facilitate a quick start by relaying information from other edges that have obtained similar optimal models. This approach allows for weighted models, reduced data return, improved model accuracy times, compared to discrete learning, and performance similar to central models.

Preliminary comprehension of the Internet of Things (IoT) is imperative prior to delving into the privacy and security concerns associated with it. In a comprehensive sense, the term "Internet of Things" refers to the worldwide network of interconnected devices that exchange information via the Internet. These devices engage in communication with one another while generating and gathering data to ensure efficient functionality.

Notably, IoT devices collect user-related information, including personal and sensitive data. Furthermore, it is essential to acknowledge that the IoT market is projected to surpass a value involves the integration of an increasing number of devices, which consequently gives rise to heightened apprehensions regarding security and privacy. The IoT domain continuously expands with the incorporation of additional devices on a daily basis. It is anticipated that approximately IoT devices will be in use worldwide recently. The escalating quantity of IoT devices is poised to bring about substantial transformations in everyday business operations. For instance, lighting systems can contribute to energy cost reduction and decreased energy consumption.

Interconnected medical devices offer benefits that enhance individuals' understanding of their health. However, these advantages come hand in hand with significant risks attributed to heightened connectivity. The proliferating number of connected devices within the IoT ecosystem creates more access points for cybercriminals and hackers, thereby raising concerns pertaining to IoT security in health related issues.

Security and privacy concerns in the realm of the Internet of Things exert a profound impact on various businesses and citizens with health monitoring. The establishment of IoT networks facilitates access to anonymous and health related

data online. If queried about the significance of security in IoT of health devices, one can point to IoT applications for patients with regular health monitoring applications.

Health monitoring entities must endeavour to enhance security measures, particularly in user-level IoT solutions, in order to foster customer trust in IoT technology in monitoring health devices. Moreover, the importance of security and privacy in the context of IoT underscores consumers' heightened awareness regarding their personal health related data. Now that an understanding has been reached regarding the vital role in security and privacy play in the long-term advancement of IoT, it is pertinent to evaluate each aspect individually for all IOT health monitoring devices. The specific security concerns are relevant within the IoT domain. As the IoT landscape becomes increasingly diverse with the advent of contemporary computing systems and advanced technologies, the vulnerability of IoT to various security threats via multiple means becomes evident.

To begin with, it is crucial to bear in mind that numerous devices within the IoT space are specifically designed for widespread deployment. Sensors are exemplary illustrations of such devices. Additionally, the deployment of IoT devices often entails a group of devices that possess similar or nearly identical features.

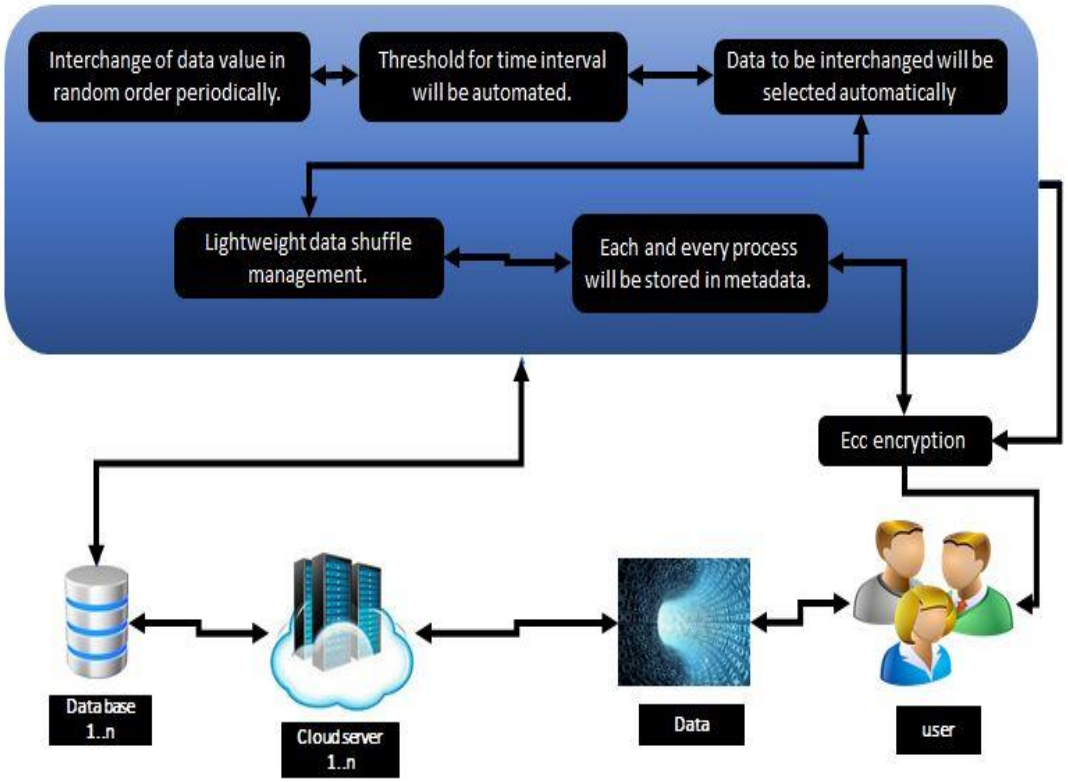

Figure 2: Server data process management.

The resemblance enhances the prevalence of these devices. While security concerns in the realm of information technology have garnered attention, the utilization of IoT introduces new challenges in health monitoring system. The importance of security in IoT stems from the reality of interaction among IoT devices. If a poorly secured device becomes connected to the IoT environment, it can compromise the security and integrity of the entire IoT system. Given the substantial quantity of homogeneous devices deployed in the IoT, both IoT users and developers must ensure that these devices do not inflict harm upon other users. It should not let the privacy data of health monitors such as blood pressure, heart rate, oxygen level etc.

Authentication stands out as one of the foremost aspects that necessitate contemplation with regard to IoT devices security. Presently employed authentication methods in IoT ecosystems only offer protection against threats such as

reverse attacks or denial of service (DoS) attacks. Furthermore, the significance of data security must be duly considered, as it represents one of the weakest areas in IoT authentication.

Various risky applications possess the capacity to amass extensive amounts of data, thereby posing severe data security risks. Additionally, with the proliferation of man-in-the-middle attacks, the importance of security becomes increasingly apparent. Third-party agents can intercept communication and assume the identity of malicious nodes participating in the exchange network. Another vital facet of the ongoing discourse surrounding IoT privacy and security pertains to how consumers perceive privacy matters.

Individuals may recognize the advantages of IoT in terms of its effectiveness in safeguarding their privacy objectives. Nevertheless, the same considerations regarding privacy and security concerns in the IoT domain can give rise to significant challenges for IoT applications in random disease check. User privacy and the right to privacy are indispensable for establishing user trust and confidence in IoT connected devices and services. Concurrently, IoT development endeavours aim to address privacy issues through innovative means.

One of the key aspects when comprehending IoT privacy issues is to consider the origins of privacy concerns. The pervasive nature of intelligent components within the IoT ecosystem enables flexible processes and distributed data from any location. The widespread connectivity inherent in IoT also plays a crucial role in accentuating privacy concerns. In the absence of specific privacy protection mechanisms, IoT connectivity can facilitate easy access to personal information from any part of the world. Armed with a clear understanding of the significance of security and privacy in the Internet of Things, it is important to identify the existing challenges. Businesses have the potential to greatly capitalize on the benefits offered by the Internet of Things (IoT). However, security threats can serve as significant barriers to the successful adoption of IoT solutions. Conversely, acquiring a comprehensive understanding of IoT security issues facilitates the development of appropriate mitigation strategies. Let us now examine some prominent issues associated with IoT security.

Insufficient Password Protection represents a prominent concern. IoT devices often possess hardcoded and embedded certificates, which render them susceptible to direct exploitation by hackers. The presence of default passwords hampers the ability of hackers to access systems. An illustrative instance of such an attack is the malware, which infected IoT devices such as routers, video recorders, and cameras. Through the exploitation of distinct types of hardcoded usernames and passwords, the malware gained control over many connected devices.

I. Health Care System With IOT Device Recommendation

Numerous industries, including healthcare, can greatly benefit from leveraging the superior performance offered by edge computing in conjunction with the cloud. Consumers can securely transmit their medical history information to doctors over the internet, which facilitates better diagnosis and care. Environmental sensors can be installed to enable doctors to remotely monitor vital signs and provide home care to chronically ill patients, as the advancements in monitoring and edge technology suggests and recommends their health oriented products. Additionally, physicians can utilize the data collected by these sensors to assess the safety of patients both inside and outside medical facilities. To ensure timely and effective patient care, data processing must be performed by end devices and nodes.

Traditional healthcare systems encounter communication issues due to organizational fragmentation and space limitations. It is crucial to establish secure platforms and applications for sharing health information, which would aid in accurate diagnoses and improved care provision. In traditional healthcare systems, doctors conduct tests and record results in tables or input them into the main database of the hospital. However, actual diagnosis becomes impractical as the main system is not connected to the user's smart phones. Clinics must retrieve a patient's complete medical record from a centralized location. Unfortunately, the confidentiality, clarity, and integrity of information are lacking, making it challenging for individuals to manage their health information.

Modern medicine relies extensively on treatment and diagnosis techniques. Electro Dermal Activity (EDA), electrocardiography (ECG), and electromyography (EMG) are utilized to detect abnormalities in the body. This process emphasizes the importance of human-based interpretation of data. Fall detection is particularly crucial for the elderly.

Furthermore, wearable devices capable of measuring parameters such as body mass index (BMI) or heart rate are now widely available at affordable prices.

Gateways are employed to receive, store, and transmit data to the required destinations. Wearables have the potential to revolutionize data collection, analysis, and processing, but they also present their own set of challenges. Various areas within the field of healthcare benefit from edge computing:

• Ambient Assisted Living (AAL): Focused on leveraging artificial intelligence to enhance health.

• Community Health (CH): Conducts health assessments of patients in public hospitals, communities, rural areas, etc.

• Semantic Medical Access (SMA): Involves extracting semantic information from vast volumes of medical data.

• Wearable Device Access: Wearable devices equipped with sensors can monitor various health parameters independently, such as heart rate, stress levels, blood pressure, blood oxygen levels, blood sugar levels, and temperature. The data can be stored in the cloud or on the internal memory of the user's smart phone.

• Mobile H-IoT: Concentrates on areas such as mobile computing and medical data collection.

• Emergency Response: Addresses challenges that can arise during emergency medical services, such as adverse weather conditions, transportation accidents, or fires.

• Children's Health Information (CHI): Provides health services to children and offers insights to caregivers regarding their health, behavioural patterns, and neurological issues.

Smart Medical Applications introduces various smart medical applications services of edge computing in smart healthcare are detailed below.

• Oxygen Saturation Monitoring (OSM): A pulse oximeter continuously measures blood oxygen saturation. The collected data is transferred to cloud storage using Bluetooth technology.

• Electrocardiogram (ECG) Check: The electrocardiogram machine is a crucial tool for recording and monitoring heartbeats.

• Blood Pressure Level Sensor: A smart terminal tracks the user's location using IoT networks, and the recorded data from sensors is transmitted to the network via a communication module.

• Temperature Monitoring: Body temperature can be measured using the integrated temperature sensor of TelosBmote.

• Diabetes Test: An important medical application for diabetics and the elderly.

• Rehabilitation Approach: Isolates patients with various physical or mental illnesses in treatment centres and aids in their recovery.

• Wheelchair Transport: Intelligent wheelchair management assists people with disabilities by intelligently following their movement patterns.

• Mobile H-IoT: This IoT paradigm combines smart phone capabilities with IoT functionality, providing mobile medical services. Medical and fitness apps monitor real-time vital signs and offer advice on weight management, diet, and nutrition.

• Future Medical Applications: Skin disease treatment, eye disease detection, haemoglobin level measurement, abnormal cell growth identification, peak flow rate (PEFR) assessment, cancer diagnosis, and remote surgery are some of the potential medical applications in the future.

I. EDGE SYSTEM WITH TRANSFER LEARNING

Transfer learning is a methodology that focuses on utilizing diverse knowledge transfer techniques at the core to address distinct yet interconnected tasks at the target, even in the absence of consistent information and considering the distribution characteristics of training and testing problems. This application of adaptive learning models at the periphery of the network to enhance performance and reduces communication latency across various servers. Any extensive system involved with embedded systems is regarded as a high-performance system. Embedded systems are specifically designed to execute specific microprocessor-based tasks while operating with limited resources and low power consumption. They possess a functional map and multiple environmental states to generate significant outcomes.

In terms of the end connection, it is crucial to define the activities and dynamics of the external environment. To provide further clarification, conducted tests on a link using edge devices and learning process represent the end network, and in

a particular region to compare the latency of the transfer learning model. Consequently determined the modified model performs well and reflects actual reality.

Global health encounters periodic occurrences of pandemics, with the current scenario being the outbreak of the pandemic disease. The particular disease exhibits a highly contagious nature and spreads rapidly. Within a span of six months since the first reported case, a substantial number of individuals across multiple countries have been infected, and the contagion continues to propagate. The existing healthcare systems are ill-equipped to handle such pandemics at certain stages, necessitating the utilization of resources for mitigation purposes.

The utilization of adaptive learning models on edge networks surpasses on-premises systems in terms of cost, performance, and efficiency. Concurrently, the contemporary era heavily relies on Artificial Intelligence (AI) and data science, where Deep Learning (DL) stands out as one of the prominent methodologies. DL can play a crucial role in mitigating pandemics like COVID-19 by addressing various aspects such as curbing the spread, disease diagnosis, drug and vaccine discovery, treatment methodologies, patient care, and more. However, the implementation of DL necessitates extensive datasets and powerful computational resources. One commonly observed challenge is the dearth of reliable datasets during ongoing pandemics. Hence, the application of Deep Transfer Learning (DTL) becomes highly effective, as it leverages knowledge gained from one task and applies it to another.

Furthermore, in a pandemic situation, the utilization of Edge Devices (ED), such as Internet of Things (IoT) devices, web cameras, drones, smart medical equipment, and robots, proves to be invaluable. These devices enhance the sophistication and automation of healthcare infrastructures, thereby aiding in managing outbreaks effectively. However, EDs possess limited computational resources, posing a challenge when employing DL. Therefore, the use of DTL becomes particularly advantageous in such scenarios. This article conducts a scientific examination of the potential and challenges associated with these issues. It provides an in-depth analysis of the technical background relevant to the subject matter and reviews the current state of the art. Moreover, the article outlines the DTL pipeline implemented over Edge Computing as a prospective avenue for pandemic mitigation assistance in the future.

The advancements in computing power and response time are establishing new benchmarks in current and future treatments. Prior edge Computing was utilized but suffered from inefficiencies in data transfer, slow response time, and limited service capabilities. The increase in data transmission costs is primarily attributed to delays caused by network congestion. While Cloudlet based solutions offer lower latency compared in edge they lack the required mobility due to limited availability of Wi-Fi networks. Several studies have compared the resources of cloud based and edge based computing and concluded that only edge computing can effectively address the present demands for latency, mobility, and energy usage.

The Internet of Things (IoT) in telemedicine generates an unprecedented amount of data that needs to be transmitted, analysed and stored. Utilizing cloud computing to process such large volumes of data leads to unacceptable data latency and high storage costs. Consequently, edge computing is employed alongside the cloud, allowing users in proximity to the data-generating nodes to address these issues in a 5G environment with the aid of intelligence. The application of edge computing and artificial intelligence in telemedicine for remote healthcare and automated disease diagnosis integrates various technologies such as computer science, medicine, and communication. This integration aims to enhance patient treatment efficiency and reduce treatment costs.

Telemedicine represents a contemporary medical service model that caters to the time-sensitive monitoring and health management of individuals in the comfort of their homes, thereby reducing outpatient visits to hospitals. Given two prevalent global trends the aging population and the increasing pace of modern life healthcare has become a concern for society as a whole. The aging population, in particular, will face challenges in accessing medical care at hospitals in the future. Additionally, the impact of the fast-paced lifestyle on the health of young individuals is becoming more significant. To address these health problems, a deep integration of the medical and healthcare industry with advanced technologies such as the Internet of Things, 5G, artificial intelligence, big data, and cloud computing is necessary. Notably, the Internet of Things and the intelligence facilitated by 5G continue to support novel applications in the field of telemedicine.

Telemedicine application scenarios in healthcare and medical science primarily encompass remote monitoring, remote ultrasound, remote consultation, remote surgery, mobile health, smart drug management, self-management tools, and access to medical information management. Biomedical wearable devices for monitoring vital signs are currently experiencing rapid development, with low cost, low power consumption, compact size, and intelligence being crucial factors. Wearable health devices offer advantages such as continuous medical services, real-time comprehension of

medical information, and proactive detection of early signs, enabling individuals to take better care of their health and understand their bodies. Advanced semiconductor technology has reduced the cost and power consumption of traditional devices while significantly enhancing their performance. The combination of artificial intelligence and the Internet of Things has further augmented the intelligence of wearable devices. Consequently, the research and development of wearable biomedical equipment has become a vital factor in the field of telemedicine.

To ensure rapid progress in telemedicine, wearable devices pertaining to healthcare should constitute a significant portion of wearable equipment. In recent years, 5G networks have attracted considerable interest across various sectors due to their high-speed connectivity, great connectivity, and low latency. The high-speed capabilities of 5G enable support for high-definition remote communication (e.g., 4K/8K) and rapid transmission and sharing of medical data. Professionals can engage in consultations anytime and anywhere, enhancing accuracy, guidance, and the connection of quality medical equipment to patients' homes.

The extensive connectivity capabilities of 5G allow for the connection of numerous medical sensors, video equipment, and biomedical wearables. This facilitates the identification, measurement, capture, and continuous transmission of medical information, thereby enabling individuals to access their health information without being limited by time or location. Specialty hospitals like radiology hospitals and medical centres can also employ medical staff to control the transportation of paramedics to designated beds within the protected area.

Various medical instruments, biomedical equipment, and health indicators (e.g., body temperature, heart rate, blood pressure, diabetes, ECG) can be monitored in real time. These devices can be connected wirelessly. Furthermore, AI analysis of health related data is performed to record patients' health status, provide disease analysis for doctors and patients, and assist in decision-making. Doctors can analyse patients' conditions and offer immediate health advice. Some healthcare providers can locally analyse data without relying on cloud connectivity.

For instance, a heart monitor equipped with automated health data analysis can promptly alert caregivers when a patient requires assistance. The extensive use of IoT devices in the medical field results in the generation of substantial data, including sensitive and time-critical health information. Due to the limited computing, storage capacity, and power of IoT devices, implementing IoT-based telemedicine applications locally at the terminal is not feasible. However, transmitting all health data to the cloud places significant stress on cloud infrastructure and poses challenges in terms of network bandwidth and end-to-end latency. Additionally, cloud computing centres are unable to provide location-aware applications.

5G-based edge computing offers an improved network architecture infrastructure for telemedicine. Edge computing brings computing, storage, and other infrastructure resources closer to end users or data sources. It extends the concept of cloud computing to the edge of aggregation, such as base stations. Edge computing encompasses computing, storage, networking, and application capabilities at the edge of the network, with network capacity being one of its primary resources. Notably, edge offers decentralization, data localization, and low latency. The combination of edge, transfer learning and telemedicine is crucial. However, to meet the requirements of diverse scenarios, close coordination between edge computing and cloud computing is necessary to maximize the benefits of both cloud computing and edge services. Data collected from medical and health-related equipment is transmitted to the edge computing server for local processing, analysis, and storage. Emergency documents are time-stamped, analysed, and immediately responded to. Since most data is not stored in the central cloud, end-to-end latency and reverse link bandwidth are reduced. Nevertheless, this does not imply the exclusion of cloud computing facilities from the telemedicine process. Certain data still needs to be transmitted from edge nodes to the cloud computing centre.

Cloud computing centres perform big data analysis, mining, data sharing, and concurrent training and updating of AI algorithm models. They push the learned or updated AI models to the edge, enabling real-time decision-making based on the health information of end nodes. Moreover, medical and health information needs to be stored in the cloud to ensure storage reliability and facilitate information sharing.

Prominent technology companies play a crucial role in the installation and implementation of intelligent purification systems due to their business benefits. For instance, IBM invested $1 billion in 2014 to establish the Watson business unit. IBM Watson employs artificial intelligence to comprehend complex data patterns. Currently, this system is utilized in the diagnosis and treatment of tumours, heart diseases, diabetes, and other areas. The first artificial intelligence product in medicine incorporates image recognition, deep learning, and medical expertise. It assists doctors in diagnosing cancer,

enhancing scanning accuracy, and supporting real-time analysis. It also facilitates early screening for lung cancer, diabetic retinopathy, breast cancer, and other diseases.

Various studies have proposed innovative systems that leverage deep learning, cloud computing, and edge computing in the field of telemedicine. These systems employ sensors to capture electroencephalogram (EEG) signals, transmit them to edge devices, distribute them for pre-processing, and then forward the enhanced signals to cloud computing servers. The cloud servers employ deep models to extract deep features from the EEG signals, determine whether a person is normal or pathological, and disseminate the results to relevant parties. Other research focuses on techniques such as Edge Learning-as-a-Service (Edge LaaS) for processing local health assessment data and healthcare for rural patients based on smart home IoT devices.

Current automated algorithms for ECG analysis primarily rely on the examination of morphological features. However, recent advancements in pattern recognition have enabled researchers to utilize deep learning techniques such as convolution neural networks (CNN) and recurrent neural networks (RNN) to process biomedical signals. CNNs have been used for the detection of premature ventricular contractions and human identification from ECG signals. Additionally, recurrent neural networks, such as the trace-based recurrent neural network have been proposed for the automatic diagnosis of acute myocardial infarction.

The telemedicine services to users by monitoring their physical parameters in real time and predicting their health status through the utilization of IoT, edge server, and machine learning technologies. The system leverages the analysis of health and user environment data, including electrocardiogram (ECG) data, global positioning data (GPS), weather information, and temperature information. In the edge computing layer, data is first collected and then analysed using AI technology to derive health indicators. Since most physical measurements monitored by the system originate from essential to achieve rapid and accurate self-diagnosis and analysis of ECG behaviour for the entire system.

Hence, an AI-based ECG testing model is employed in the edge computing layer to improve the overall system performance. After data analysis, test results and health information are sent to the cloud server for storage and management. By placing the convolution neural model within the MEC layer, the proposed system fully capitalizes on the advantages of this method and provides users with real-time cardiac diagnosis.

I. EXPERIMENTAL RESULTS

The provided pseudo code offers a comprehensive system for data collection and uploaded from a specific device, emphasizing robust data privacy measures. It comprises various functions that collaboratively facilitate data processing and transmission. The "collectAndUploadData(device)" function orchestrates data collection, followed by anonymization, culminating in the upload of anonymized data to a cloud edge system. The "anonymize(data)" function ensures data privacy by removing personally identifiable information (PII) through "preserveIdentity(data)" and "maintainAnonymity(data)" sub-functions. In case of an emergency condition, the "alertEmergencyCondition(condition)" function queries essential services from the edge system and processes requirements using the "swiftQueryServices()" function.

The system then executes actions based on the required services via functions such as "performActions(requiredServices)" and "edgeSystem.completeActions(requiredServices)." Data is securely stored and transferred within the edge system using functions like "edgeSystem.uploadData(data)" and "edgeSystem.transferLearning(data)." User privileges are managed by functions such as "grantPrivileges(user)" and "grantPrivilegesBasedOnCategory(user)." Additionally, the system handles personal data access through functions like "handlePersonalData(user)" and "accessDataWithLogin(user)." It ensures data authenticity with the "authenticateAndAccessData(user)" function. Emergency information can be shared with officials through the "shareEmergencyInfoWithOfficials(info)" and "shareInfoWithOfficials(info)" functions. Finally, the system determines the best edge system through "chooseBestEdgeSystem()" and "selectBestEdgeSystem()" functions based on predefined criteria.

The provided pseudocode outlines a sophisticated system for data collection and uploads from a designated device, encompassing stringent data privacy measures. Below is a technical pseudo code:

```
BEGIN
  FUNCTION collectAndUploadData(device)
  data = device.collectData()
  anonymizedData = anonymize(data)
  cloudEdgeSystem.uploadData(anonymizedData)
  FUNCTION anonymize(data)
  anonymizedData = preserveIdentity(data)
  anonymizedData = maintainAnonymity(anonymizedData)
  RETURN anonymizedData
  FUNCTION preserveIdentity(data)
  preservedData = applyPreservationTechniques(data)
 RETURN preservedData
 FUNCTION maintainAnonymity(data)
 anonymizedData = removePII(data)
 RETURN anonymizedData
 FUNCTION alertEmergencyCondition(condition)
 IF condition
 requiredServices = swiftQueryServices()
edgeSystem.processRequirements(requiredServices)
 FUNCTION swiftQueryServices()
requiredServices = edgeSystem.queryServices()
RETURN requiredServices
FUNCTION processRequirements(requiredServices)
actions = edgeSystem.completeActions(requiredServices)
RETURN actions
 FUNCTION edgeSystem.queryServices()
categorizedData = categorizeData()
RETURN categorizedData
FUNCTION categorizeData()
categorizedData = performCategorization()
RETURN categorizedData
FUNCTION edgeSystem.completeActions(requiredServices)
actions = performActions(requiredServices)
RETURN actions
FUNCTION performActions(requiredServices)
```

actions = executeActions(requiredServices)

RETURN actions

FUNCTION edgeSystem.uploadData(data)

edgeSystem.storeData(data)

FUNCTION edgeSystem.storeData(data)

edgeSystem.transferLearning(data)

FUNCTION edgeSystem.transferLearning(data)

edgeSystem.saveDataInLocation(data)

FUNCTION edgeSystem.saveDataInLocation(data)

savedData = saveData(data)

RETURN savedData

FUNCTION saveData(data)

savedData = saveDataBasedOnFrequency(data)

RETURN savedData

FUNCTION saveDataBasedOnFrequency(data)

savedData = saveDataWithFrequency(data)

RETURN savedData

FUNCTION grantPrivileges(user)

privileges = grantPrivilegesBasedOnCategory(user)

RETURN privileges

FUNCTION grantPrivilegesBasedOnCategory(user)

privileges = assignPrivileges(user)

RETURN privileges

FUNCTION handlePersonalData(user)

personalData = handleDataWithLogin(user)

RETURN personalData

FUNCTION handleDataWithLogin(user)

personalData = accessDataWithLogin(user)

RETURN personalData

FUNCTION accessDataWithLogin(user)

personalData = authenticateAndAccessData(user)

RETURN personalData

FUNCTION authenticateAndAccessData(user)

personalData = authenticateUser(user)

RETURN personalData

FUNCTION shareEmergencyInfoWithOfficials(info)

shareInfoWithOfficials(info)

FUNCTION shareInfoWithOfficials(info)

officials.shareInfo(info)

FUNCTION chooseBestEdgeSystem()

bestEdgeSystem = selectBestEdgeSystem()

RETURN bestEdgeSystem

FUNCTION selectBestEdgeSystem()

bestEdgeSystem = determineBestEdgeSystem()

RETURN bestEdgeSystem

END

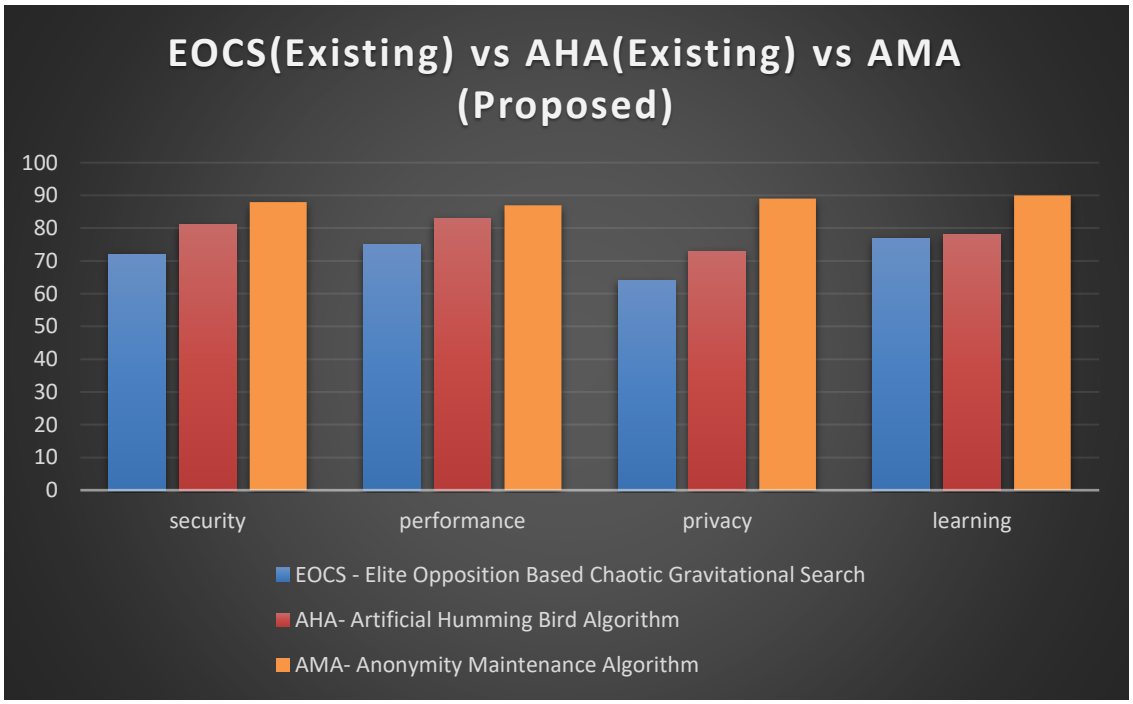

Figure 3. Graph Comparing Existing methods vs Proposed Method

The above graph compares the performance of the existing Artificial Humming Bird Algorithm (AHBA) with the proposed Anonymity Maintenance Algorithm (AMA) across four key metrics: Security, Performance, Privacy, and Learning. The X-axis represents these four metrics, while the Y-axis indicates the measured values in percentage.

Security: The "Security" dimension assesses how well each algorithm protects data from unauthorized access and ensures the confidentiality of sensitive information. A higher percentage on the Y-axis implies stronger data security capabilities for the respective algorithm.

Performance: The "Performance" aspect evaluates the computational efficiency and speed of each algorithm in handling data anonymity tasks. Higher values on the Y-axis indicate superior performance, with faster processing times and reduced computational overhead.

Privacy: The "Privacy" metric gauges the extent to which each algorithm safeguards individuals' personal information while maintaining data utility. A higher percentage on the Y-axis denotes more effective data privacy preservation.

Learning: The "Learning" dimension refers to the algorithms' adaptability and ability to improve over time by learning from past data. A higher value on the Y-axis indicates greater learning capability and potential for enhanced data anonymity.

The graph features two distinct lines, one for AHBA and the other for AMA. Each line showcases the respective algorithm's performance across the four metrics at various levels of data complexity. As we examine the graph, we can interpret and draw conclusions based on the following observations:

The AMA's line consistently stays above the AHBA's line across all four metrics, it indicates that the proposed AMA outperforms the existing AHBA in terms of security, performance, privacy, and learning capabilities.

The AMA's line demonstrates a steeper upward trend compared to the AHBA's line in any metric, it suggests that the AMA offers more significant improvements in that particular aspect.

The AHBA's line remains close to or overlaps with the AMA's line, it implies that the two algorithms exhibit similar performance in that specific dimension. Any line shows fluctuations or plateaus in certain metrics areas of improvement. Ultimately, the graph aids in understanding how the proposed AMA compares to the existing AHBA in crucial aspects of data anonymity. It provides valuable insights for decision-makers and developers in choosing the most suitable algorithm for specific data privacy and security requirements.

I. CONCLUSION

In conclusion, the proposed system for IoT devices introduces a comprehensive approach to data collection, anonymity and privacy preservation. By swiftly querying service availability during emergencies and efficiently triggering actions without revealing personal identities, the edge system ensures effective response and user protection. Categorization techniques aid in eradicating unwanted data, while transfer learning facilitates efficient data storage and management. Enhanced security is achieved through granted privileges and stringent authentication standards. Overall, the proposed concept offers a robust solution for safeguarding user data and integrity in the dynamic realm of IoT devices. This anonymity maintenance from IoT devices in the edge system will be achieved successfully.

REFERENCES

[1] J. Vaidya, Clifton. "Protection safeguarding affiliation rule mining in vertically divided information" In: Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. Edmonton, Alberta, Canada: ACM.2002:639-644.

[2] C. Yao, "Conventions for secure calculations," Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science, IEEE Press, New York, 1982.

[3] Gui Qiong, Cheng Xiao-Hui. Affiliation Rule Mining Algorithm Based on Similarity Matrix of Transactions [J]. Diary of Guilin University of Technology, Vol. 28, No.4, Nov.2008, p. 568-571.

[4] Mahmoud Hussein, Ashraf El-Sisi, Nabil Ismail, "Fast Cryptographic Privacy Preserving Association Rules Mining on Distributed Homogenous DataBase", Knowledge-Based Intelligent Information and Engineering Systems, Lecture Notes in Computer Science, Volume 5178/2008, pp. 607 - 616 (2008).

[5] Chris Clifton, Murat Kantarcioglu, Jaideep Vaidya, Xiaodong Lin, and Michael Y. Zhu (2003), "Apparatuses for security saving appropriated information mining," SIGKDD Explorations, Vol. 4, No. 2pp1-7.

[6] Shamir;"How to share a mystery," Communications of the ACM, vol.22 (11), pp.612–613, 1979.

[7] Jaiwei Han and Micheline Kamber, "Information Mining Concept and Techniques", Morgan Kaufman Publishers, second Edition, 2006.

[8] Moez Waddey, Pascal Poncelet, Sadok Ben Yahia, "Novel Approach For Privacy Mining Of Generic Basic Association Rules, "In PAVLAD'09, November 6, 2009, Hong Kong, China, 2009 ACM.

[9] Xuan Canh Nguyen, Hoai Bac Le, Tung Anh Cao, "An Enhanced Scheme For Privacy-Preserving Association Rules Mining On Horizontally Distributed Databases," In 2012 IEEE.

[10] N.V. Muthu Lakshmi1 and K. Sandhya Rani, "Protection Preserving Association Rule Mining in Vertically Partitioned Databases," In International Journal of Computer Applications (0975 – 8887) Volume 39– No.13, February 2012.

[11] Xinjing Ge, Li Yan, Jianming Zhu, Wenjie Shi, "Protection Preserving Distributed Association Rule Mining Based on the Secret Sharing Technique," 2009 IEEE.

[12] Zhu Yu-quan, Tang Yang, Chen Geng, "A Privacy Preserving Algorithm for Mining Distributed Association Rules," 19-21 May 2011

[13] Dean, J. and Ghemawat, S. MapReduce: simplified data processing on large clusters. Communications of the ACM 51 (1) (2008) 107-113.

[14] Zaharia, M., Chowdhury, M., Das, T., Dave, A., Ma, J., McCauley, M. and Stoica, I. Resilient distributed datasets: A fault-tolerant abstraction for in-memory cluster computing. Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation, 2012, 2-2.

[15] Power, R. and Li, J. Piccolo: Building Fast, Distributed Programs with Partitioned Tables. OSDI 10 (2010) 1-14.

[16] Malewicz, G., Austern, M.H., Bik, A.J., Dehnert, J.C., Horn, I., Leiser, N. and Czajkowski, G. Pregel: a system for large-scale graph processing. Proceedings of the ACM SIGMOD International Conference on Management of data, 2010, 135-146.