Journal of Information Systems Engineering and Management
2026, 11(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Federated AI Based Learning Platform through Protecting Data Privacy and Security for Heterogeneous Data

Saikrishna Tipparapu

Independent Researcher, USA Senior Cybersecurity Engineer

ARTICLE INFO

Received: 06 Aug 2026

Revised: 26 Sept 2026

Accepted: 06 Oct 2026

ABSTRACT

This paper proposes a Federated Learning Secure Approach (FLSA) to enhance data privacy and security in IoT-based healthcare systems. By integrating encryption and privacy-preserving mechanisms, the framework ensures secure data processing and sharing, reducing latency and improving scalability. Performance analysis demonstrates the framework's reliability in maintaining data accuracy while minimizing service overhead. Those data's need reliable and secure communication as it is the details with more confidential data also as it helps to develop an automated and secure communication in the field of healthcare. In the advanced era, confidential data's being generated from the IoT devices are deployed in distributed manner. In order to secure the user information's, it needs strength user privacy policy as it helps to have customized network infrastructure and it is applicable for various advance application in real time especially for healthcare. To preserve the user policy, the federated learning will act as the machine learning to optimize the data being offered to deploy smart cities. In this paper, FL based Secure Approach is proposed which is enabled with federated learning and encryption policy, which is enabled with user privacy preservation especially for automated healthcare application. In this approach, security and privacy is ensured by applying the environment of encryption based on complex data in cloud. Instead of sending the user personal data to the cloud platform, this approach makes those user data to be learned using federated machine learning technology. In the performance analysis, service overhead is being calculated based on the probability of services offered and its service reliability is analysed. Thus, this proposed approach makes the latency to be reduced based on the storage requirement.

Keywords: Encryption, Federated learning, Internet of Things, Healthcare, Privacy and Security.

I. INTRODUCTION

Federated Learning (FL) makes to analyse the machine learning input data as it extracts those data related to various sources. This learning model makes to associate with multiple organization data sources to perform knowledge discovery with keeping the data to in the distributed environment [1]. This FL provides to improve the model as it takes the data from various Internet of Things (IoT) devices along with local trained data from the model. In recent days, all the services are made as digital one as it requires lot of data to be generated from multiple IoT devices. Emerging technologies like Artificial Intelligence (AI) and IoT based models make certain use cases to develop smart cities and make improved and effective healthcare applications with smart methodologies [2]. These smart technologies are associated with Machine Learning (ML) and Deep Learning (DL) models as it plays a significant role to perform data extraction and those extracted data helps to make certain effective predicted decision in the organization. As FL gets originated at 2016 as it makes the data to be loaded and associated with other system locally. In the initial state, the single federated help to provide the improvement towards the model globally as the data's are generated by the devices are it is associated with the model locally developed [3].

In the field of health care based IoT, loT based data's are available and those data's are much useful for the medical industry. In the recent days, deep learning based approaches are being used as it helps the IoT-based healthcare to process effectively by automating the data accuracy and the medical condition of the patients are monitored effective and continuously and having added with artificial intelligence. In order to identify and diagnosis the condition of the patient as it applied with recent deep learning approaches as it makes decrease in the patient waiting time [4]. This

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

IoT based Healthcare makes the process of generating and collecting the data as they are sensitive and confidential. To ensure data guarantee and privacy to protect the confidential data and secure the quality data required.

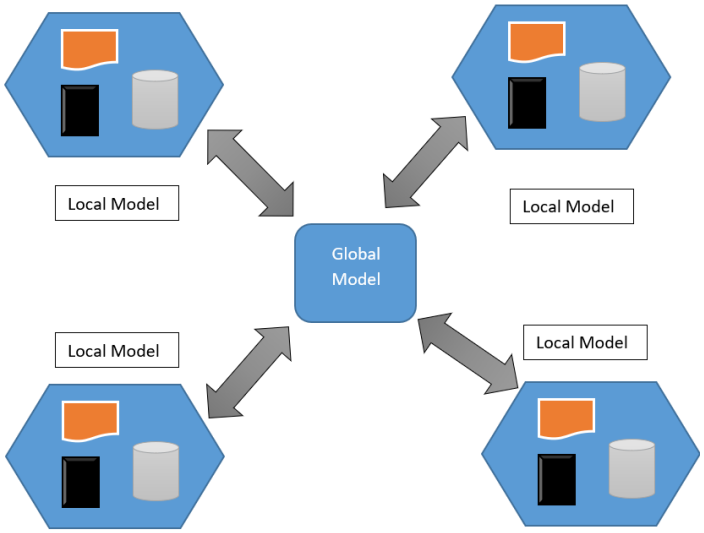


Figure 1. FLSA System Architecture: This diagram integrates IoT devices, encryption modules, and cloud servers to ensure secure data sharing and processing

In the healthcare based IoT, deep learning-based approaches has been proposed in various scenerios as it helps to ensure security and privacy of the data. The combined way of training the data is not bargained as for that the researcher as proposed various various approaches [5]. [6] has proposed the method, which considers the data leakage privately as it is integrated with Federated Learning and auhor has analysis and measure the data trust ability based on various metrics like, provisioning the data to ensure data privacy and data complication. As this model is not suitable with a large sum of data [6], quantitative analysis of the data reliability and trust ability is maintained based on certain security metrics [7] as this model is included with enhancement in the data privacy and complication. Then above models are associated with FL concept as it represents the data privacy degree over certain data as it improves in training the data as the illegitimate user not able to access the confidential data. [8] propose the model based on weighted FL as it suitable for multi-party user as they perform computation based protocol to perform encryption process on the data. As the existing FL based model not suitable for ensuring security in the confidential data of healthcare. All the confidential data are attached with the centralized cloud server as there is a possibility on cloud attacks and it results in some critical issue and challenges on those data i.e. information loss. So, the privacy plays a significant role on the medical field especially on the confidential data as they are more sensitive for the patients on the hospital [9].

A method to safeguard against privacy intrusions is differential privacy (DP), which involves the intentional adding of disturbance to the training updates by each site. Nevertheless, although this paradigm safeguards private information, it incurs a utility trade-off and may result in less efficient AI models, as evidenced by recent studies. A further privacy-preserving method applicable to SMPC is homomorphic encryption (HE). HE can guard against a hostile server eavesdropper while preserving AI model performance by encrypting weight updates before transmitting them to the central server. A popular technique for implementing HE in machine learning is fully homomorphic encryption (FHE), in which every operation is carried out in an encrypted environment.

Subsequent studies expanded upon CKKS by incorporating additional modules, including bootstrapping and novel batching procedures, to enhance performance and reduce computational time. Although CKKS-based software programs offering a high level of privacy assurance, they are computationally intensive to run, which causes a severe shortage of resources during SMPC training, especially with massive amounts of records. Conversely, none of the studies utilized extensive real-world medical datasets to validate their methodologies, leaving their practicality and computing demands in the realm of medical image analysis ambiguous. This technology, known as somewhat

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

homomorphic encryption (SHE), has their possibilities to alleviate processing demand or risking anonymity for specified steps in the process.

The main objective of FL is to integrate with Machine Learning (ML) / Deep Learning (DL) protocol as it helps to generate the data using IoT on the Model locally. Based on the association of DL, latency reduction and bandwidth can be applied as it makes the data images to be moved from one node to another node as they faces the problem of risk security and these problems can be solved using Federated Learning. As the nodes present on the networking environment are dynamic as they are supported with FL as they are resulted with over crowed area with these nodes as they make FL to enhance further.

Here, in this paper various challenges related to security and privacy on healthcare data systems are discussed and it helps to proposed the framework with the integration of Federated learning and block chain as it provides ensure on data privacy and security, which helps to improve the data scalability with the use case study. The performance analysis is done on the various metrics such as,

The paper is organized as follows,

II. LITERATURE SURVEY

The role of FL is used for various applications such as medical-based healthcare, restaurant, etc. generally, FL takes role to collect and generate data from various mobile devices as they are stored on the cloud as they are updated. It takes the recent advantages as they collect the data from mobile devices as they are trained by ML/DL model and get updated [10]. In the medical field, data security and privacy factors play a significant role. Privacy on the data is more important as there are more confidential data are considered. In medical applications, patient data's are increasing more and more as they lead to the possibility of performing attacks on those data. In order to avoid the outside activities of the malicious users, the process of encryption and authentication plays a significant role. The various attacks such as, eavesdropping, replay attack, Denial of Services, Distributed Denial of Services, etc. as they provides threat to the data specific to the healthcare applications [11].

In this existing system of data, is used vastly on many real-time applications as they are unprotected by illegitimate users. It contains some confidential data as they need to be protected based on the integration of FL and those data need to be trained by the global model. In some cases, FL makes it comprise security as few malicious users can get into the system [12]. In order to address the issue of security, the encryption is considered as it gives some significant solutions as it is associated with ML/DL models as they are able to train the data and get stored and it helps to enhance the data security [13]. As the encryption takes the decentralized framework, FL takes to integrate the encryption as it helps to improve the effectiveness of the data consensus on the encryption. In this case, FL takes some extension as it supports the distributed environment and it takes the ML/DL algorithms to train the data, which are stored on various devices such as mobile phones, laptops, etc.

The mobile devices perform certain learning model as it update the data with certain data exchange and verifying as they are influenced more on encryption technology [14]. They have certain characteristics such as, distributed environment, authentication, data mutability, decentralized mechanism, etc. as these characteristics are used for the healthcare applications as they gives improved solutions for data security and privacy [15]. [16] has discussed the role of Artificial Intelligence on the medical data of healthcare applications. The medical data's are ensured with privacy and security as it is integrated with federated learning for medical healthcare applications. The FL takes the compromise on the data security as they certain malicious users are attacked on the system data. [17] has proposed the security architecture as it overcome the problem of data security into the next level as the federated learning is integrated with encryption in the cloud environment as it leads to data scalability, security and privacy. Various challenges and issues related to data security and privacy are discussed with the integration of federated learning [18 - 22].

In order to guarantee the performance factors such as, data confidentiality, data integrity and authentication, the [23] and [24] has proposed the framework with encryption as it protects the data privacy in a trusted environment but this framework is not suitable for multi-party environment. So, further the model has been proposed as it uses encryption as the data can be shared and secure based on the IoT devices through multiple service providers as it

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

enables the shared data transfer among the multiple users. Then the limitations of FL with encryption makes secure data with the factor of reliability and data accountability as they influence the decentralized framework of encryption as they update the model performance effectively [25]. The various factors of healthcare data with FL takes certain challenges and issues are addressed in [26-29] as it takes the integration of FL and encryption.

From the above existing literature survey, it is concluded that the federated learning and encryption gets a space to work with IoT devices to gather the data and secure & process it effectively.

III. SOCIETAL AND GLOBAL BENEFITS:

Ensuring compliance with legislative frameworks like as HIPAA and GDPR is of the utmost importance for the healthcare business. This is particularly true when using technologies such as Federated Learning and Artificial Intelligence. Healthcare professionals have used AI-based models to evaluate data collected by IoHT devices and successfully treat a range of illnesses. Legal requirements and rules like HIPAA and GDPR say that data must be processed and analysed in a way that doesn't violate privacy.

Many entities can collaborate to train an ML model without sharing data thanks to a machine learning-based technique known as federated learning (FL). It is particularly beneficial in the healthcare sector, where privacy and data security are important factors. FL does, however, address several privacy concerns; IoHT data privacy guarantees are still pending formal demonstration. Privacy-enhancing technologies (PETs) aim to improve online communication and data security. In order to make appropriate decisions in the healthcare industry, healthcare organisations train ML-based models in clouds or data centres utilising data provided by IoHT devices. However, due to direct access limits and laws (HIPAA and GDPR), these models face performance issues due to limited data availability on a centralised server for training.

As a result, the models that are produced can prove to be biassed and untrustworthy. Despite sufficient data, training on a centralised server needs significant resources, leading to high costs and hindering application in many hospitals and research organisations. The safeguarding of personal data from unlawful use and manipulation is feasible through the implementation of data privacy protection. We must adhere to ethical privacy regulations throughout the data lifecycle while collecting and storing patient data. To safeguard privacy at the data level, the GDRP and HIPAA privacy policies are examples of legislation. Patient health data is accessible exclusively to authorised individuals in accordance with privacy policies.

So, an IoHT system needs to be built with the following rules in mind to protect patient data privacy:

Smart healthcare systems have traditionally relied on centralised AI functions in the cloud or data centres for health data learning and analytics. Given the increasing amounts of health data and the proliferation of IoMT devices in current healthcare networks, this centralised approach is inefficient in terms of communication latency caused by raw data transmission and cannot achieve high network scalability. Furthermore, the reliance on a central server or third party for data learning creates serious privacy concerns, such as user information leakage and data breaches. This is especially true in e-healthcare, where health-related information is very sensitive and confidential due to regulations like HIPAA. Furthermore, in the future healthcare systems, it is possible that such a centralised AI architecture will no longer be acceptable. This is since health data are not located in an isolated spot but rather are disseminated across a large-scale IoMT network. As a result, there is an urgent need to use distributed AI techniques to enable scalable and privacy-preserving intelligent healthcare applications at the network edge.

Given this, federated learning (FL) has become a viable option for implementing smart healthcare systems that are more affordable while maintaining better privacy protection. FL is a distributed AI technique that enables the training of high-quality AI models by aggregating local updates from numerous health data clients, such as IoMT devices, without requiring direct access to the local data. This could restrict the disclosure of sensitive user information and preferences, reducing the danger of privacy leakage. Furthermore, because FL attracts large computation and dataset resources from several health data clients to train AI models, the health data training quality, e.g., accuracy, would be significantly improved, which could not be achieved by using centralised AI approaches with less data and limited computational capabilities.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A. Key Challenges In Iot Data Security And Privacy:

The healthcare industry is especially vulnerable to cyberattacks and data breaches due to the interconnection of healthcare systems and the rising usage of EHRs. Data breaches can risk patient privacy and security and undermine public trust in healthcare companies. AI systems frequently use large datasets and complex algorithms, which may need careful explanation. The primary impediment to successful federated learning is weight updates. When the deep learning model for medical image analysis optimises during the training phase using backpropagation, this problem occurs.

Due to site-specific differences in hardware, operating systems, and network conditions, learning algorithms must function across multiple platforms. This makes implementing federated learning challenging. Disparities in image acquisition procedures and tagging techniques throughout universities present another difficulty. The IoT attack surface is expanding on a daily basis as an increasing number of devices are brought online, including our smartwatches, smart TVs, smart homes, and smart vehicles, as well as the growing industry IoT. In addition to consumer items, IoT sensors are widely employed in healthcare, manufacturing, and supply chain activities, as well as green agriculture, economics, and national defence.

Burgeoning IoT encompasses virtually any device or sensor that is connected to the internet, ranging from a large container on an ocean barge to a tiny Tile Tracker for your phone. For example, according to the IEEE IoT technology projection, the number of linked devices will rise from 8.7 billion in 2020 to over 25 billion in 2030, a 300% increase. Given the extended attack surface for security risks to availability, integrity, and confidentiality, organisations must prioritise IoT security in order to secure their network environments from IoT device-borne threats.

IV. RESEARCH METHODOLOGY

In this research work, managing the resource problem is considered and the ownership data gets enabled based on federated learning and encryption. As the data is combined with encryption, sample data (SD_i) is loaded with the miner.Here the mobile devices are formed as the multiple clusters as represented as, $\{L_1, L_2, L_3, \ldots L_L\}$ as it belongs to Data in the image. Data 'D' degree represents the data load 'D_L' as those data's are enabled with federated learning. In a particular case, when the mobile devices access the data as mentioned as M_k belongs to DS as DS = L_K; From the multiple cluster $\{L_1, L_2, L_3, \ldots L_L\}$, L_L = degree(M) as moner will be selected. As we have uses encryption technology and it follows decentralized environment, the data's gets trained as it considers the problem of data regression and the loss function gets reduced by solving the above problem based on the data samples. It makes the data to be pre-processed, the mean square error is calculated. In this article, apart from the above problem of regression, the privacy issue also been considered and ML/DL makes data pre-processing process and FL is applied with the proposed one. Based on the integration of FL and encryption, the data being processed for data sharing and exchanging.

The FLSA system architecture takes the platform of cloud as the service with the integration of IoT and Encryption. The architecture is classified into, Sensor Networks as the data centres as private as it stores the data, which are generated by the IoT devices. The stored data being stored into the cloud network as it makes some process of data validation and process and then it will be moving to the data monitoring and other healthcare equipment. Based on the sensor nodes, such as, temperature, heartbeat, ECG, oximeter, etc. whenever the particular services being initiated, required data being processed and sent from the cloud server. The specific parameters such as, CPU, computational power, GPU, etc. are requested by the services and it is determined based on the demand. In the architecture, the cloud server and data are being connected with the encryption and its main role is to establish the secure communication and compute the data effectively.

1. IoT Devices:

- Role: Generate raw data streams, including health monitoring sensors.

- Text Addition: "The framework begins by acquiring data from IoT sensors such as heart rate monitors, temperature sensors, and smartwatches."

2. Gateways:

- Role: Serve as intermediaries for secure data transmission.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Text Addition: "Gateways handle encryption and secure communication between devices and the federated learning platform."

A. Encryption with Data Aggregation and Association

These encryption data's are stored based on the process of aggregating the data and associating with them and ensure data authentication. In the data processing, the user applies to the targeted data and that particular data's are processed and attains the particular results. The secure communication is established based on the permission and control given to the data and the data is labelled with quality level after the particular data is trained and processed. Then the trained data with the label is sent to the FL model and the data labels are,

- To the datasets, the data labels are assigned
- Assign the label, console is used
- To label the data, human are handled

B. Federated Learning (FL) based Prediction Process:

In FL, the data results are taken from the data users in the data center. Then the computational logic takes technique and data analyser prediction process based on the present and past history of data lines. This prediction process takes to improve the system outcome results.

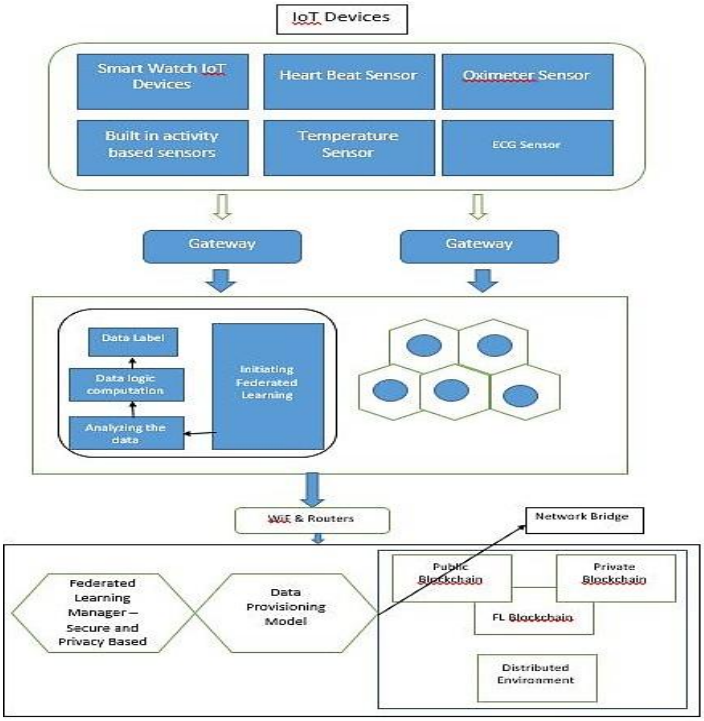


Figure 1. Proposed FLSA System Architecture

In Figure 1, IoT devices such as, smart watch, Heartbeat, Oximeter, Buit In activity based sensors, Temperature and ECG helps to collect the data information related to the users. Then FLSA architecture performs by taking the input from the IoT devices via Gateway. As the input is taken into the system as it enters to the federated learning gets initiated. In the federated learning gets up 3 phases as mentioned below,

1. Analyse the data
2. Logic Computation on data
3. Label those data

The above phases are repeated for all the data and via Wi-Fi / Routers, federated learning data requires data to be gets security and privacy. As those data helps to perform provisioning based on the model as it takes up the provisioning based on network bridge. Here, learning manager takes blockchain as it takes up the private and public blockchain as it gets integrated with federated learning blockchain in the distributed environment.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

In this data processing, a modified reward function is used to determine the data accuracy and minimize the energy and latency. The reward function is represented as in Figure 2 and formulated below,

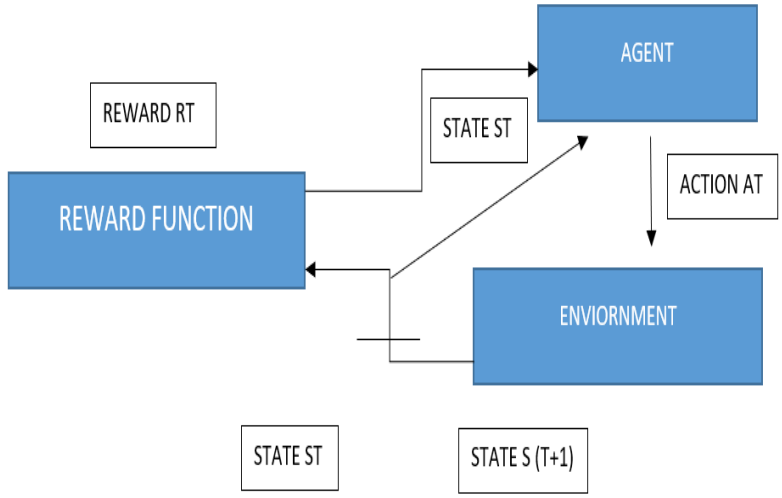


Figure 2. Reward Function

Reward Function (RF) $\Pi_*(t|b) = \arg\max V_\Pi (t, b)$ ---------- (1)

Algorithm 1: Modified Reward Function

Input: Optimal Value (O_V)
Output: Determine the maximum value function'

```
1.  Defining the function for Optimal Value (OV)
2.  While True
3.      Learning = 0; // Data learning assigned as NULL value
4.      For t in range (env. nB)
5.          Quality.tb = np.zero (env. nb) // To check the data quality based on the encrypted
    data
6.          For b in range (env. nB)
7.              For prob_t, next state, Reward function, _in env.P[t][b]
8.                  Q_tb[b] +=Prob_t * (reward + gamma * v[nest_state]
                        // Data Quality determined based on the Reward
                          function and Gamma with state defined.
9.          Maximum value Function_t = np.max(Q_tb) // Determine the maximum value
    function
```

Then the trained data is generated in the encryption. In the healthcare system, the registered data are configured using the encryption and moved to the private encryption and then the data owner will check. While performing the data transaction and collaboration, the data being shared with other users are get authorized in the healthcare application. While performing the communication, security is established and an authentication approach is applied to the healthcare information. Then the data are secured and protected in the distributed environment in order to offer trust ability and security solutions.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

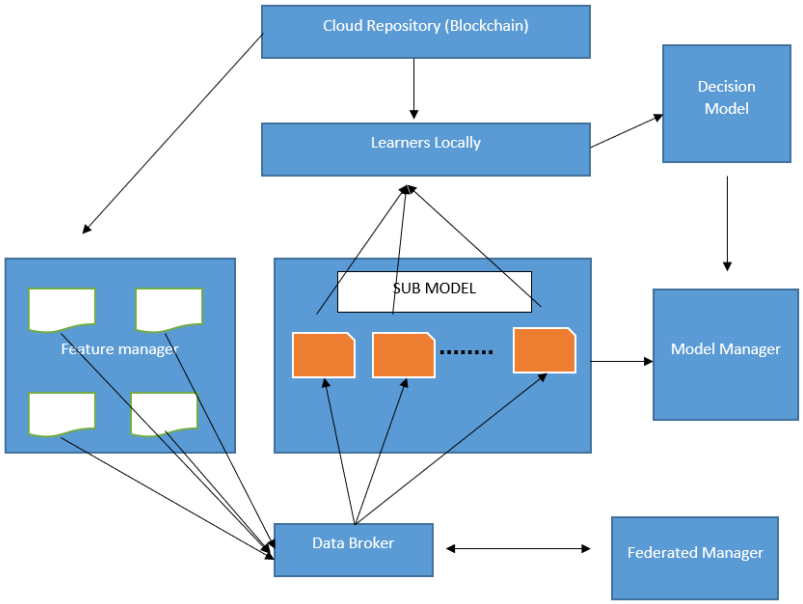


Figure 3. FL Based Secure Architecture using Encryption

C. Secure Federated Learning:

In this prediction process, protection-based privacy mechanism is discussed in Figure 3 as it contains various sub models such as, gesture, voice and handwriting, etc. The data aggregation is performed on the federated manager and in the federated manager the learners get spited based on the leaners for certain real time applications. Based on the federated learning, each sub datasets are trained using the sub-models DL/ML. In order to sort out the problem of privacy, process of coalition is performed. FL integration helps to reduce the risk occurs in the confidential data's of healthcare applications. The computation of multi-party is performed to secure the data based on cryptographic function with private data in the encryption.

V. VULNERABILITY IDENTIFICATION MODULE

Based on the module, various vulnerability gets identified as such denial of service and information disclosure vulnerabilities. To mitigate the vulnerability and ensure security to the data being generated.

Algorithm: Vulnerability Identification Module

Input: Initialise the FL based architecture

Output: Identify the vulnerability

The proposed FL based architecture being chosen
Initialize the Matrix

Construct the test case generation {t_1, t_2, t_3, … t_n}

{

Identify the Recognised Data with vulnerability

}

Test case generated

Monitoring the packet communication process

{

Apply the application based on Security Communication protocol

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

}

Construct the breakpoints during the communication process

Perform monitoring based on abnormality

Identify the data with vulnerability

In the above algorithm, proposed architecture is chosen for the test experiment and initialize the matrix. This matrix generated helps to make test case construction / generated as it takes the vulnerable data as the input to make the data processing. Then test case makes some monitoring as it takes security-based communication protocol, and it helps to monitor the data transmission process. This process makes to identify the vulnerability at the certain point as it makes some break point at some communication point. Based on the above process, vulnerability in the data packets in the communication gets identified.

VI. PERFORMANCE ANALYSIS

In the performance analysis, FL based Secure Approach is proposed to secure the data communication and perform data pre-processing with training process based on DL/ML algorithm. In Table 1, the data loss is calculated based on the process of training phase for the proposed system and it performs a gradual increase in the value based on the variation in the iteration from 0 to 500.

Table 1. Number of Iteration Vs. Data Loss

S. No.	Number of Iteration	Data Loss (Training Process)
1	0	0.00075
2	100	0.00096
3	200	0.00156
4	300	0.00321
5	400	0.00386
6	500	0.01056

In the Table 2, the data accuracy is determined based on the training process by varying the number of iterations from 0 to 500. The data accuracy of the proposed FLSA gets decreases gradually and the average value of 92.5. In Table 3, the data accuracy is determined based on the training process by varying the number of iterations 0 to 500 based on the testing process. The data accuracy of the proposed FLSA gets decreases gradually and the average value of 0.925.

Table 2. Number of Iteration Vs. Data Accuracy (Training Process)

S. No.	Number of Iteration	Data Accuracy (Training Process)
1	0	95.5
2	100	91.8
3	200	89.8
4	300	93.6
5	400	90.6
6	500	90.1

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 3. Number of Iteration Vs. Data Accuracy (Testing Process)

S.No.	Number of Iteration	Data Accuracy (Testing Process)
1	0	0.925
2	100	0.922
3	200	0.924
4	300	0.892
5	400	0.886
6	500	0.869

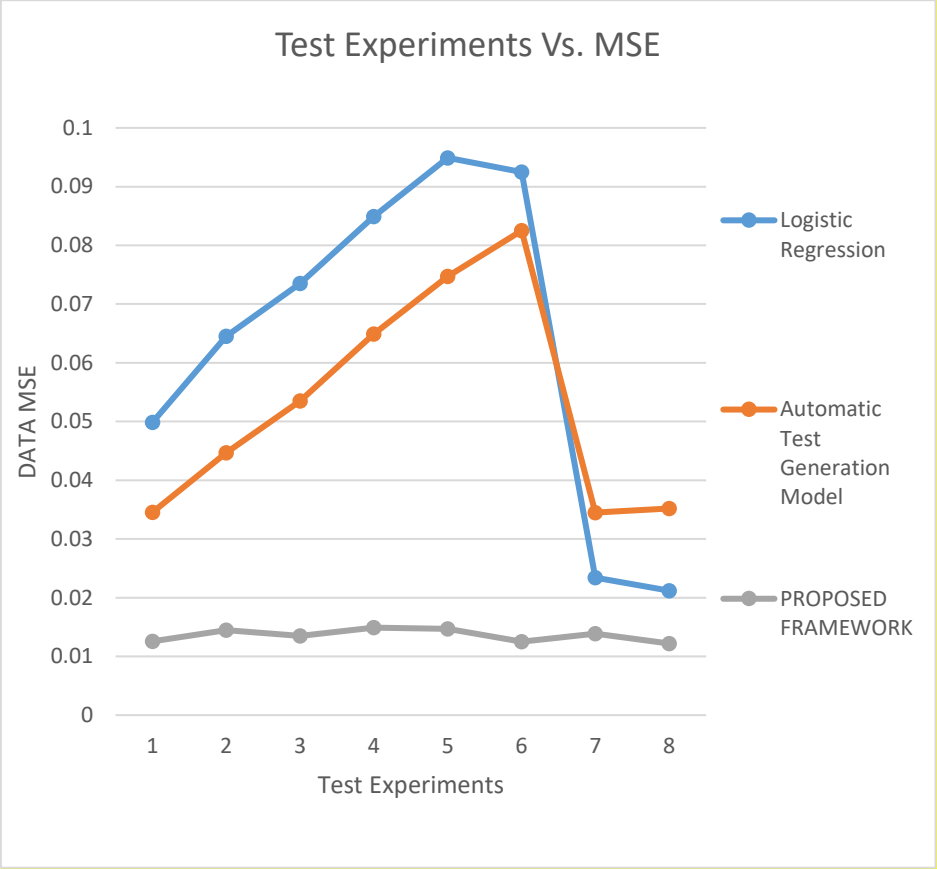


Figure 4. Test Experiment Vs. Data MSE

In the above Figure 4, Mean Square Error (MSE) is calculated based on the varies test experiments are conducted from 1 to 8. Then the proposed model has obtained decrease in the error value as compared to the existing models such as, logistic regression and automatic test generation model.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2026, 11(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

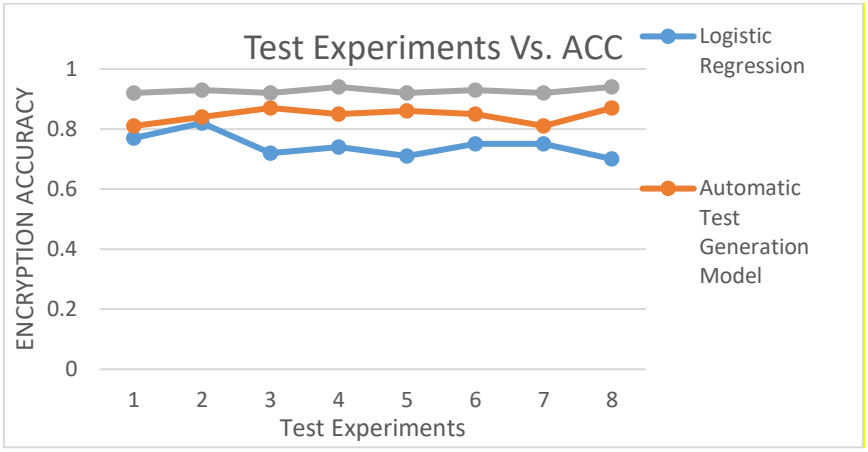


Figure 5. Test Experiment Vs. Encryption Accuracy

In the above Figure 5, Accuracy (ACC) is calculated based on the varies test experiments are conducted from 1 to 8. Then the proposed model has obtained increased in the accuracy value as compared to the existing models such as, logistic regression and automatic test generation model.

Based on the Figure 4 & 5, proposed framework gets enhanced in terms of security and reliability based on the data being generated.

VII. CASE STUDIES BASED ON IOT BASED HEALTH CARE:

The case studies being discussed below as follows based on healthcare,

A. Philips Healthcare's IntelliVue Guardian Solution uses IoT devices and cloud computing to monitor patients in real time. Cloud-based wearable sensors and monitoring equipment are linked. Continuous monitoring is done on vital signs like blood pressure, heart rate, and respiration rate. Healthcare professionals receive immediate alerts in the event of abnormal readings, and the data is uploaded to the cloud for processing. This enhances patient outcomes and permits early intervention [46]. Care station Insights: This GE Healthcare product uses IoT and cloud technologies to improve patient care and anaesthesia delivery.
Sensor-equipped anaesthesia devices collect data on patient vital signs, gas levels, and machine operation. The cloud receives this data for analysis. Anaesthesiologists can make better decisions, optimise anaesthesia delivery, and enhance patient safety by using the system's real-time information.

B. IBM Watson Health - Watson for Oncology: Description: Cloud-based artificial intelligence (AI) helps oncologists make treatment decisions. Watson for Oncology analyses patient data, including medical records, research papers, and clinical trial information, to offer personalised treatment options. This cloud-based AI technology enables oncologists to stay up to date on cancer research and make informed treatment decisions.

C. Proteus Digital Health - Digital Medicine System: Description: Proteus Digital Health is a Digital Medicine System that is particularly beneficial for medication adherence. It is created by combining IoT and cloud technology. A pill with a tiny sensor is taken by the patient. A wearable patch that tracks when the medication is taken is in communication with this sensor. Patients and healthcare professionals may track medication adherence in real time thanks to data that is sent to the cloud. For the management of chronic diseases, this method is especially helpful [46].

D. Connected Asthma Inhalers: Overview: Several businesses, such as Propeller Health and AstraZeneca, have created connected inhalers to treat asthma. Patients' usage patterns are monitored using IoT-enabled inhalers. Information about medication adherence and environmental factors influencing asthma symptoms is provided by the data, which is transferred to the cloud. Then, using the individualised data, medical professionals can modify treatment regimens.

E. Vivify Health provides remote patient monitoring using IoT devices and cloud-based analytics. Patients use IoT devices like tablets, wearables, and biometric sensors to monitor their health from home. Data is sent to

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

the cloud so that medical professionals can view it instantly. Readmissions to hospitals are decreased because of proactive care management for patients with chronic illnesses.

These case studies demonstrate how Cloud-IoT applications in healthcare can improve patient outcomes, enhance treatment decisions, and enable personalised and efficient delivery. These illustrations show how IoT devices, cloud computing, and analytics can be used practically to address a range of healthcare issues.

VIII. CONCLUSION

Federated learning is integrated with machine learning in order to ensure security and privacy in order to improve scalability and latency. The main objective of FL is to integrate with Machine Learning (ML) / Deep Learning (DL) protocol as it helps to generate the data using IoT on the Model locally. Based on the association of DL, latency reduction and bandwidth can be applied as it makes the data images to be moved from one node to another node as they faces the problem of risk security and these problems can be solved using Federated Learning. As the nodes present on the networking environment are dynamic as they are supported with FL as they are resulted with over crowed area with these nodes as they make FL to enhance further. FL based Secure Approach is proposed to secure the data communication and perform data pre-processing with training process based on DL/ML algorithm. In Table 1, the data loss is calculated based on the process of training phase for the proposed system and it performs a gradual increase in the value based on the variation in the iteration from 0 to 500. In Future work, other ML/DL algorithms can be used to improve the scalability and latency further.

REFERENCES

[1] J. J. Kang, ``Systematic analysis of security implementation for Internet of health Things in mobile health networks,'' Springer Nat. Data Sci. Cybersecurity Cyberthreat Intell., vol. 1, no. 1, pp. 87 -113, 2020.

[2] M. S. Hossain, M. A. Rahman, and G. Muhammad, ``Cyber-physical cloud-oriented multi-sensory smart home framework for elderly people: An energy effciency perspective,'' J. Parallel Distrib. Comput., vol. 103, pp. 11-21, May 2017, doi: 10.1016/j.jpdc.2016.10.005.

[3] V. Balasubramanian, M. Aloqaily and M. Guizani, "A Federated Learning Secure Encryption Framework for Autonomous Systems," IEEE International Conference on Communications, ICC, 2024, DOI: 10.1109/ICC51166.2024.10622293.

[4] Ethem Alpaydin, Introduction to Machine Learning, MIT Press, 2020.

[5] V. Sharma, I. You, K. Andersson, F. Palmieri, M.H. Rehmani, J. Lim, Security, privacy and trust for smart mobile-internet of things (M-IoT): A survey, IEEE Access 8 (2020) 167123-167163.

[6] W.Y.B. Lim, N.C. Luong, D.T. Hoang, Y. Jiao, Y.C. Liang, Q. Yang, D. Niyato, C. Miao, Federated learning in mobile edge networks: A comprehensive survey, IEEE Commun. Surv. Tutor. (2020).

[7] N. Li, M. Xu, Q. Li, J. Liu, S. Bao, Y. L, J. Li and H. Zheng, "A review of security issues and solutions for precision health in Internet-of-Medical-Things systems," Security and Safety, Vol. 2, 2023. DOI: 10.1051/sands/2022010.

[8] G.A. Kaissis, M.R. Makowski, D. Rückert and R.F. Braren, "Secure, privacy preserving and federated machine learning in medical imaging," Nature Machine Intelligence, Vol. 2, pp. 305-311, 2020, DOI: 10.1038/s42256-020-0186-1.

[9] F. Marulli, E. Bellini and S. Marrone, "A security-oriented architecture for federated learning in cloud environments," Workshops of the International Conference on Advanced Information Networking and Applications, Springer, Cham, pp. 730–741, 2020. DOI: 10.1007/978-3-030-44038-1_67.

[10] Z. Li, V. Sharma and S.P. Mohanty, "Preserving data privacy via federated learning: Challenges and solutions," IEEE Consumer Electron. Mag. Vol. 9, Issue. 3, pp. 8–16, 2020. DOI: 10.1109/MCE.2019.2959108.

[11] S. Singh, P.K. Sharma, B. Yoon, M. Shojafar, G.H. Cho and I.H. Ra, "Convergence of Encryption and Artificial Intelligence in IoT Network for the Sustainable Smart City," Sustainable Cities and Society, p. 102364, 2020. DOI: 10.1016/j.scs.2020.102364.

[12] P. K. Sharma, J. H. Park, and K. Cho, "Encryption and federatedlearning-based distributed computing defence framework for sustainablesociety," Sustainable Cities and Society, vol. 59, p. 102220, 2020. DOI: 10.1016/j.scs.2020.102220.

[13] X. Lu, Y. Liao, P. Lio, and P. Hui, "Privacy-preserving asynchronousfederated learning mechanism for edge network computing," IEEEAccess, vol. 8, pp. 48970–48981, 2020. DOI: 10.1109/ACCESS.2020.2978082.

[14] X. Zhao and C. Huang, "Microservice based computational offloading framework and cost-efficient task scheduling algorithm in heterogeneousfog cloud network," IEEE Access, vol. 8, pp. 56 680–56 694, 2020. DOI: 10.1109/ACCESS.2020.2981860.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

[15] A. Lakhan and X. Li, "Transient fault aware application partitioningcomputational offloading algorithm in microservices based mobilecloudlet networks," Computing, vol. 102, no. 1, pp. 105–139, 2020. DOI: 10.1007/s00607-019-00733-4

[16] N. Bouacida and P. Mohapatra, "Vulnerabilities in Federated Learning," IEEE Access, Vol.9, pp. 63229 – 63249, 2021. DOI: 10.1109/ACCESS.2021.3075203

[17] G. Tsoumplekas, C. Athanasiadis, D. I. Doukas, A. Chrysopoulos and P. Mitkas, "Few-Shot Load Forecasting Under Data Scarcity in Smart Grids: A Meta-Learning Approach," Energies, MDPI, Vol.18, Issue. 3, 2025. DOI: 10.3390/en18030742.

[18] V. Mothukuri, R. M. Parizi, Seyedamin Pouriyeh, Yan Huang, Ali Dehghantanha and G. Srivastava, "A survey on security and privacy of federated learning," Future Generation Computer Systems, Vol. 115, pp. 619-640, 2021. DOI: 10.1016/j.future.2020.10.007.

[19] S. Almutairi and A. Barnawi, "Federated learning vulnerabilities, threats and defenses: A systematic review and future directions," Internet of Things, Vol. 24, 2023. DOI: 10.1016/j.iot.2023.100947

[20] Naranjo, María Maestre, Santos, Claudio Paya, Alonso, Silvia Arranz, Alos, Lucia Granados, Pineda, Neidy Zenaida Domínguez, Rey, Manuel Nevado, Fernández-Rodríguez, Juan Carlos, Workplace Aggression Against Healthcare Workers: A Cross-Sectional Registry Study Comparing Primary and Specialized Care, Advances in Public Health, 2026, 5959054, 8 pages, 2026. https://doi.org/10.1155/adph/5959054

[21] D. Zhu, J. Chen, X. Zhou, W. Shang, A. E. Hassan and J. Grossklags, "Vulnerabilities of Data Protection in Vertical Federated Learning Training and Countermeasures," IEEE Transactions on Information Forensics and Security, Vol. 19, pp. 3674-3689, 2024, DOI: 10.1109/TIFS.2024.3361813.

[22] B. Jia, X. Zhang, J. Liu, Y. Zhang, K. Huang and Y. Liang, "Blockchain-Enabled Federated Learning Data Protection Aggregation Scheme With Differential Privacy and Homomorphic Encryption in IIoT," IEEE Transactions on Industrial Informatics, Vol. 18, Issue. 6, pp. 4049-4058, 2021.

[23] E.M. Abou-Nassar, A.M. Iliyasu, P.M. El-Kafrawy, O.Y. Song, A.K. Bashir and A.A. Abd El-Latif, "DITrust chain: towards encryption-based trust models for sustainable healthcare IoT systems," IEEE Access, Vol. 8, pp. 111223-111238, 2020. DOI: 10.3390/en18030742

[24] X. Guo, H. Lin, Y. Wu and M. Peng, "A new data clustering strategy for enhancingmutual privacy in healthcare IoT systems," Future Gener. Comput. System, Vol. 113, pp. 407–417, 2020. DOI: 10.1016/j.future.2020.07.023.

[25] M.A. Almaiah. F. Hajjej, A. Ali, M.F. Pasha and O. Almomani, "A Novel Hybrid Trustworthy Decentralized Authentication and Data Preservation Model for Digital Healthcare IoT Based CPS," Vol. 22, Issue. 4, 2022. DOI: 10.3390/s22041448.

[26] W. Zhang, D. Yang, W. Wu, H. Peng, N. Zhang and H. Zhang, "Optimizing Federated Learning in Distributed Industrial IoT: A Multi-Agent Approach," IEEE Journal on Selected Areas in Communications, Vol. 39, Issue. 12, pp. 3688-3703, 2021. DOI: 10.1109/JSAC.2021.3118352.

[27] V. Puri, A. Kataria and V. Sharma, "Artificial intelligence-powered decentralized framework for internet of things in healthcare 4.0," Trans. Emerg. Telecommun. Technol, pp. e4245, 2021. DOI: 10.1002/ett.4245.

[28] S.P. Kumar, J. H. Park and K. Cho, "Encryption and federated learning-based distributed computing defence framework for sustainable society," Sustainable Cities Soc. Vo.. 59 pp. 102220, 2020.

[29] L.N. Bao, E.L. Lydia, M. Elhoseny, I. P.,Denis A. Pustokhin, M.M. Selim, G.N. Nguyen, and K. Shankar, "Privacy preserving encryption technique to achieve secure andreliable sharing of IoT data," Comput. Mater. Contin. Vol. 65, Issue. 1, pp. 87–107, 2020. DOI: 10.32604/cmc.2020.011599.

[30] A. Yazdinejad, A. Dehghantanha, H. Karimipour, G. Srivastava and R. M. Parizi, "A Robust Privacy-Preserving Federated Learning Model Against Model Poisoning Attacks," IEEE Transactions on Information Forensics and Security, Vol. 19, pp. 6693-6708, 2024. DOI: 10.1109/TIFS.2024.3420126.

Copyright © 2026 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.