International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (Online): 2347-5552, Volume-13, Issue-6, November 2025
DOI: https://doi.org/10.55524/ijircst.2025.13.6.17
Article ID IJIRE-1420, Pages 159-168
www.ijircst.org

Secure Aggregation and Differential Privacy for Legally-Compliant Machine Learning on Community-Wide Infectious Disease Data

Gnanesh Methari[1] and Dr Iqra Rasool[2]

[1] Department of Information Technology (Cybersecurity), Franklin University, Columbus, United States
[2] Department of Hematology, Chughtai Institute of Pathology, Lahore, Pakistan

Correspondence should be addressed to Gnanesh Methari; Metharignanesh770@gmail.com

Received: 2 November 2025 Revised: 16 November 2025 Accepted: 29 November 2025

ABSTRACT- The dramatic increase in community-wide infectious disease data - generated by electronic health records, mobile health applications and public health data reporting systems has created opportunities in machine learning (ML) like never before, to assist with predicting outbreaks, monitoring diseases and taking community health-related actions. But due to the sensitive health data, privacy, security, and legal issues are high. The classical centralized method of ML creates a risk of revealing personally identifiable information and can be not in accordance with the new regulations such as GDPR and HIPAA. To overcome these issues, privacy-saving methods, including secure aggregation and differential privacy, have become the key to the implementation of legalization of ML on distributed health data. The review critically reviews the principles, applications and limitations of these techniques as they are applicable to infectious disease analytics. It summarises prior studies on secure aggregation protocols, differential privacy schemes and federated learning designs, demonstrating the contribution each contributes to the privacy of sensitive health information and the utility of models. Also, the review emphasizes the fact that there are certain key challenges, i.e., scalability, the problems of accuracy-privacy trade-offs, and integration with legal frameworks, and indicates the directions that should be followed in the future research to enhance the technical and regulatory compliance. The content of the review is expected to inform the researcher, policymakers, and practitioners on how to create effective, secure, and ethically responsible strategies to community-wide surveillance and analysis of infectious diseases through the use of ML, as it offers a general idea about the current approaches to privacy protection in the context of big data and analytics practice.

KEYWORDS- Federated Learning, Differential Privacy, Secure Aggregation, Privacy-Preserving Machine Learning, Infectious Disease Surveillance, Public Health Data, Outbreak Detection, Data Privacy and Security

I. INTRODUCTION

A. Global Infectious Diseases and the Need for Community-Wide Data

Globally, infectious diseases continue to pose an issue in terms of health in the population [1]. Such diseases as Covid-19, Influenza, Dengue, and Mpox continue to impact numerous states at the same time [2]. There are some diseases that fall temporarily, only to reoccur or in other regions. The future outbreaks also place the world at risk due to climate change, population movement and new strains of the virus.

The recent statistics about health in the world, and not limited to the region, show that there are cases of infectious diseases. They are instead found in most regions of the world and they affect them in varying degrees. This implies that disease surveillance should not be done on individual level but at a community and population level.

In the below figure 1 provides an international accounting of the reported infectious disease cases in six regions of World Health Organization network: Europe, Western Pacific, Americas, South-East Asia, Eastern Mediterranean and Africa (during the period, late January to February 2023). The number of the cases per day with time and the regional distribution of the cases percentage is shown in Panels A, B, C and D respectively.

Comprehensively, the data prove that infectious diseases are common and exist at the same time in various regions. The greatest cases reported in this period are Western Pacific and Europe. In Panel B, the Western Pacific area has slightly more than half of the total reported cases, and next is Europe, thus more than a third. Americas also have a significant contribution with South-East Asia, Africa and the Eastern Mediterranean having lesser proportions.

The A and C panels depict important daily changes in the number of cases. It is possible to observe several sharp peaks especially in Western Pacific, Europe and Americas. These extreme upward movements pull these indicators to signal an outbreak event or reporting of surging upwards and not real disease level. Other regions on the other hand have lower but maintained levels of cases indicating that infectious diseases are also still present in the areas even at relatively low levels of cases.

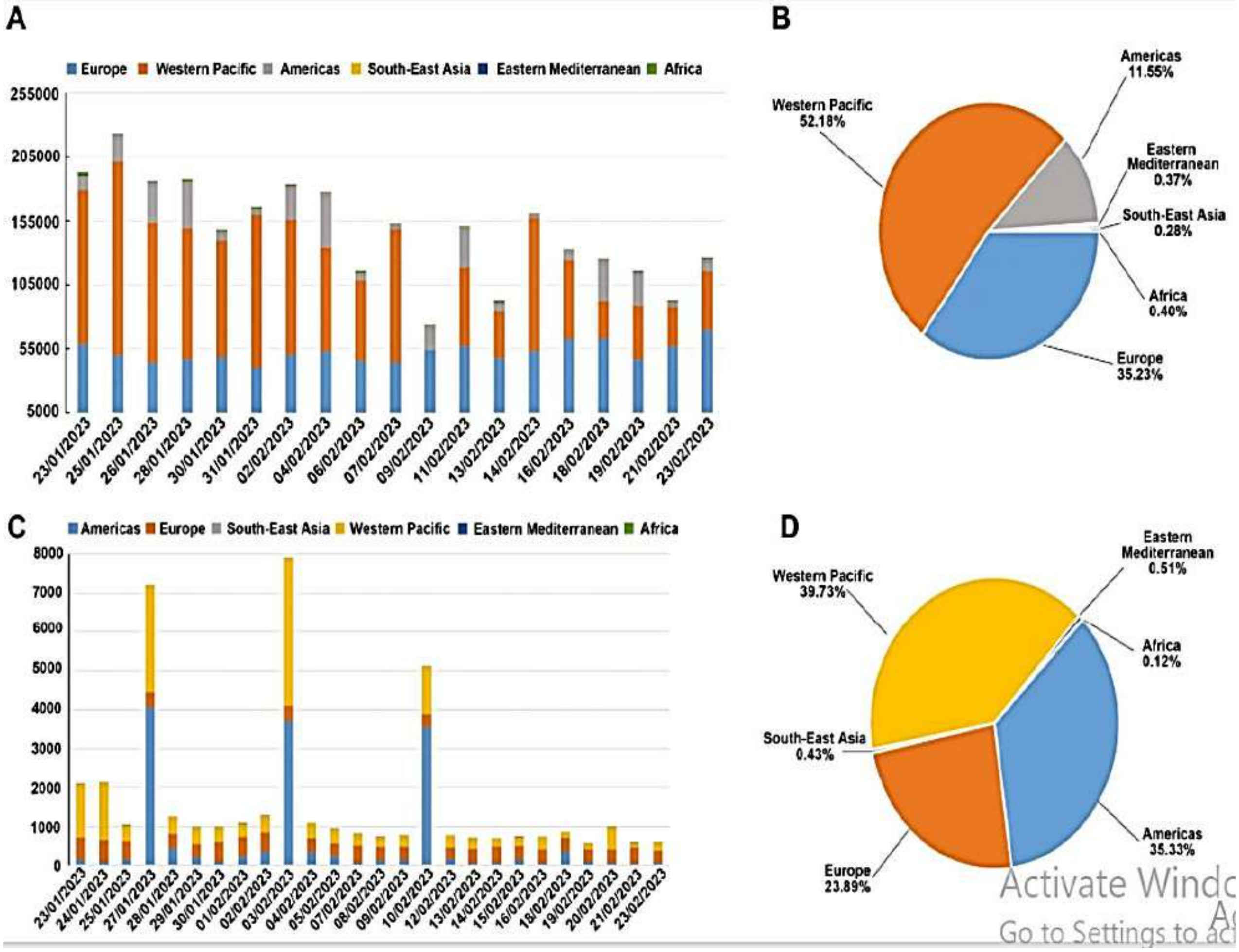


Figure 1: Global infectious disease trends across regions during January–February 2023

Panel D also throws more weight on the non-uniform distribution of the disease burden on the regional basis. The number of cases is high in some areas but low in others yet all the areas are not free of infectious diseases. This unequal distribution represents variations in the number of people, surveillance capacity, risks to local and risk of exposures to diseases.

Combined, the figure demonstrates that the number of infectious diseases in the month of February 2023 was not only worldwide and a community-wide issue, it was not merely something confined to one nation or the entire planet. These trends state the requirement of continued data collection and analysis on the international front. They also show that large-scale, privacy-preserving data sharing is required to be effective in infectious disease surveillance and early warning systems and coordinated responses of the population health.

B. Machine learning in surveillance of Infectious Diseases

Machine learning is widely applied in the sphere of public health because of the abundance of the existing health data. The disease spread is predicted with the help of the ML models and identification of the risk groups of people [3]. These models can be used to enhance the decision-making process as well as to assist health authorities to react quicker to outbreaks.

Nonetheless, the majority of ML systems continue to use a centralized data collection [4]. This implies that the information of the hospitals, clinics as well as the mobile devices is relayed to a central server. Although the practice is applicable in training of the model, privacy and security risks are serious.

C. Large-Scale Health Data Privacy and Security Factors

Health information is highly confidential. Individual and behavioral data is often found in community-wide datasets [5]. Nobody can always be sure that names were removed, and people can be recognized again. Consequently, the threat of breach of privacy increases with increase in data volume.

There are also legal and ethical concerns brought up when it comes to large-scale data sharing. Such laws as GDPR and HIPAA demand the efficient protection of personal health data [6]. In case the privacy that ought to be safeguarded is lost in the eyes of the people. This could lessen inter institutional data transfer and closure of successful public health systems.

The privacy-preserving machine learning techniques have become relevant in order to overcome these problems. Federated learning allows the models to be trained without the interaction of raw data. Protecting the model updates through secure aggregation during communication [7]. Differential privacy is to restrict the opportunities of getting sensitive information based on model outputs.

The presented review is devoted to the ways these methods can be used to make machine learning of infectious disease data safe, secure, and legally compliant. It summarizes existing literature, presents issues and find out future research areas. It is intended to be used to support the responsible use of ML in community-wide infectious disease surveillance.

II. SURVEY SCOPE AND CONCEPTUAL FOUNDATIONS

A. Scope of This Review

This review is specialized in machine learning methods that protect the privacy of data related to community-wide infectious diseases. The major objective is to understand how the secure aggregation and differential privacy could provide the safety and legality of the analysis of the data. The review is grounded in the research in the machine learning, the public health and the data protection spheres.

The paper will review the subject of distributed data collection, federated learning systems, privacy risk, and legal issues. It does not present novel experiments or data sets. Besides that, it also highlights and connects research, which exists. The narrative-integrative approach is the basis of the review. This implies that it describes the ideas of what something is, compares how things are done and exposes gaps in current knowledge.

This is focused on the community-wide information, and not on single clinical studies. Data at community level plays a significant role in termination of outbreaks and monitoring the disease. Nevertheless, they present privacy threats as well. That is why these aspects as privacy and security are considered as one of the design requirements in this review.

B. Community-Wide Infectious Disease data

A vast number of sources have community-wide infectious disease data. Such entities are hospitals, clinics, laboratories, and public health agencies and the mobile health applications [8]. Part of the data is gathered on a daily basis, and at massive amounts. Certain ones are case numbers, test results, mobility patterns and symptoms reports.

One may see the changing cases of infectious diseases in the global regions in January and February 2023 using Figure 1. The greatest number of cases is in Europe and the western pacific then the Americas. There are less cases reported in South-East Asia, Africa and the Eastern Mediterranean, but cases are reported. This demonstrates that infectious diseases affect every region except that some are not affected equally.

The figure also shows that the number of cases is dynamic with time. Certain days are drastically rising and some days have less values. Such changes may be attributed to outbreaks, delays or variance in surveillance systems, or reporting. This fluctuation characterises a complicated and dynamic infectious disease data.

Due to these variations, there is no single set of data that is capable of capturing all the trends of diseases all over the world. The information is spread across territories, organizations and nations. The reporting and health policy regulations may differ in each region. This renders centralized data collection problematic and dangerous.

C. Surveillance of Infectious Diseases by Machine Learning

The method of machine learning is typically used to handle the data connected to the infectious disease. Patterns, forecasting the propagation of an illness, and assisting an early warning system can be identified with the help of ML models [9]. These tools would help the authorities in public health to make improved and quicker decisions. Conventional ML systems generally make all data be located at a central location. This is a serious challenge which is centralized. The transfer of sensitive health data to a central server will put the data at risk of being breached and misused (Seh et al., 2020). It is also a source of legal problems in case data transfers with national or regional borders.

To this, centralised learning is even harder because of the regional variation as evidenced by Figure 1. Europe, Western Pacific and American data are commonly gathered using disparate legal and technology systems. The transfer of raw data between regions may be in conflict with laws of data protection or health policies in the area. Due to this heterogeneity of the region, there is a need to have distributed approaches to learning. The federated learning allows model training in different places without exchanging raw data [11]. Individual data holders individually train the model and exchange model updates. In this manner, collaboration can be facilitated and at the same time less data can be exposed.

D. Threats in Distributed Health Data privacy

Privacy risks are even apparent in the case of federated learning. Health information is confidential and the information can still be leaked even by updating the model. The attackers can seek to infer confidential data by observing publicly available updates or model outputs [12]. In the literature, a number of threats to privacy models have been determined. These consist of inference attacks, where an attacker tries to find out whether the data of the person was used during training. The other risk is model inversion where sensitive information has been inverted into model parameters. The communication attacks may also occur when data is being transferred between the server and the client or vice versa [13].

The breach of privacy may arise in a situation where local training, model update, server aggregation, and model rerelease to users occur [14]. Without the protection of these stages, they can reveal confidential information. Secure aggregation is intended to minimize the threats of model updates sharing. It ensures the joint updates and not individual contributions can be seen by the server. Differentiation privacy is a technique of introducing noise to data or model updates so as to minimise what can be known about any given individual [15]. It is necessary to know these threat models before the implementation of privacy-preserving methodologies. Even distributed systems may have privacy law and ethical compliance breaches without express protection.

E. The Privacy Preserving and The Legal Compliant ML motivation

Since the infectious disease data currently varies at the global and the regional level as seen in Figure 1, there is the great necessity of cooperation between institutions and regions. Simultaneously, the issues of privacy and legal limitations make the scheme of sharing raw data unsafe and quite infeasible. The federated learning, secure aggregation as well as differential privacy provide a feasible resolution, they allow the training of distributed data without compromising privacy [16]. Such practices are also in line with legal principles like privacy by design and data minimization.

This review expands on these ideas to explain why safe and effective infectious disease surveillance can be achieved through privacy preserving machine learning. The following sections provide a summary of secure aggregation and differential privacy at a more detailed level, their advantages, and their weaknesses, as well as unresolved gaps in research.

III. FEDERATED LEARNING SECURE AGGREGATION

A. Meaning and Purpose of Secure Aggregation

One of the critical methods in federated learning is secure aggregation that secures sensitive data in the training of models [16]. Data may be obtained in large numbers of hospitals, laboratories, and regional health systems in community-wide analysis of infectious diseases. These data contain very sensitive data like the infection status, place, and diagnosis time. There are a significant privacy and legal risk associated with sharing such data in its raw form. Secure aggregation can solve this issue through the participation of multiple parties training a machine learning model together without disclosing their personal data or updates.

The federated learning has every participant locally training the model on its own data. Raw data is not sent to a central server but only model updates are distributed. Nonetheless, the even updates may be prone to leakage of personal information by inference attacks, or by inversion of the models [16]. Secure aggregation allows avoiding this by making sure that no participant is visible to the server but only the aggregated outcome of all updates. Consequently, each individual hospital or user cannot be recognized in the aggregate model update.

This method is particularly valuable in systems that involve infectious disease monitoring in which data are spread out geographically and are subject to various legal regulations. Secure aggregation is what allows creating a common model worldwide and retaining local data confidential and locally managed. This does not compromise privacy laws or moral principles because it allows a massive collaboration.

B. Secure Aggregation Workflow and Architecture

A typical secure aggregation process in federated learning entails a number of synchronized elements that encompass the administration of keys, local calculation, encrypted communication, and aggregation centralization [17]. In Figure 2, a secure aggregation process is illustrated, including the generation of keys, the local model training process, the sharing of encrypted updates, the cloud-based process of aggregation, and the global model update. Such a workflow will be used to make sure that sensitive health information is never shared directly, as well as the updates made to individual models are hidden.

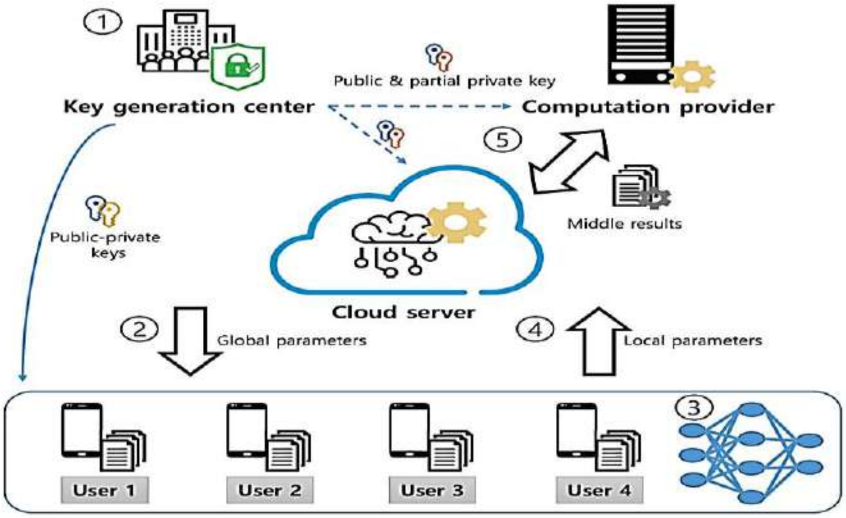


Figure 2: Secure aggregation workflow with key generation and computation provider

Federated learning is an important technique that involves secure aggregation to protect sensitive information in model training [17]. Many hospitals, labs, and regional health systems are often involved in the collection of data in community-wide analysis of infectious diseases. This information presents very sensitive data that could include but not limited to infection status, place and time of diagnosis. This type of data sharing in a raw form poses highly privacy and legal dangers. The secure aggregation addresses this problem as it allows the training of a machine learning model within a group of participants, without sharing any of their data or updates.

In federated learning, the participants are locally training the model with their data. Data is not transmitted to a central server as raw data, but rather only modifications are made in a model. Nonetheless, such updates can also be compromised by the possibility of intimate privacy breaches by inference attacks or model inversion methods [18]. Secure aggregation assists in avoiding this by making sure that the server is only provided with the aggregate of all the updates, but not the contribution by any individual participant. Consequently, the aggregate model update is not identifiable to the individual hospital/user.

This is more essential to infectious disease surveillance, where the information is spread geographically and is incongruent with legal jurisdiction. The concept of secure aggregation makes it possible to build a common global model and maintain the privacy of local data and local control over it. This is useful in assisting massive cooperation without violating privacy regulations or moral principles.

C. Aggregation Architecture and Workflow: Secure

A typical secure aggregation process in federated learning consists of a number of coordinated entities, including key management, local computation, encrypted communication and centralized aggregation [17]. Figure 2 shows a safe aggregation algorithm, which involves key generation, local model training, thoughts on encrypted updates, cloud and global model update. The flow of work guarantees the fact that no sensitive health information is shared and no model updates are ever visible.

To begin with, there is a key generation mechanism which is employed to produce cryptographic keys of the participants. These keys will allow every client to encrypt the local model update, which it will send to the server. The individual updates are not visible on the transmission and storage due to the encryption. Some systems leave control of these keys to one or more trusted or semi-trusted. It is not the case that the computation server will have access to raw updates.

Second, the training of the model is training it locally by individual participants using their own infectious disease data. This local training step is applied to extract region specific patterns like local outbreak or seasonal patterns of disease. Once the training process has been completed, the local model is used in encrypting the parameters with the assigned keys. Privacy can be ensured at this point because there are no raw data and readable updates that depart the local device or institution.

Third, the server receives encrypted updates of all participants only. It aggregates on these encrypted values directly producing an aggregated result, a learning combination of the group. Due to the encryption of the updates, the server is not allowed to view or isolate the contribution of any particular participant. Only upon aggregation, it is the final result that is decrypted in order to update the global model.

Such a workflow is capable of facilitating learning in a broad area of regions, with confidentiality of the data. The figure assists the readers of the flow of process though the overall point of the figure is widely applicable in most of the secure aggregation protocols that are applied in healthcare research.

D. Threat Models Privacy Protection

Secure aggregation aims to offer some of the most prevalent privacy threats in federated learning systems security. The honest-but-curious server is one of the greatest threats, which adheres to the protocol, yet attempts to find information in the acquired updates [19]. This threat can be mitigated using secure aggregation, where the server does not receive the update of individual values, only aggregated values.

The other threat is an inference attack whereby attackers aim at regaining sensitive information of model updates [20]. These attacks may compromise patient level information including their infection status or demographic details without protection. Secure aggregation addresses this risk by masking individual updates in a group sum, and hence it is very hard to reconstruct.

Nonetheless, the secure aggregation is not the comprehensive answer. In case participants involved in a training round are very few, then privacy assurances can be compromised. An attack on dropouts where certain clients exit the system intentionally or accidentally may also occur [21]. These constraints imply that secure aggregation should be developed sensitively and frequently paired with other methods like different privacy to provide greater defense.

E. Research Gaps, Limitations and Strengths

Obvious benefits of community-wide infectious disease modeling can be gained through secure aggregation. It enables institutions to collaborate with each other and follow data ownership principles and reduce legal risk by retaining sensitive data locally [22]. It also increases the level of trust in the people, which is necessary in massive health data initiatives. Simultaneously, there is additional overhead in computation and communication on the part of the aggregation. Complexity of the system also includes encryption and management of keys that are not simple to the low-resource healthcare setting [23]. Scalability is the other problem when there are thousands of people.

Future studies address the enhancement of the protocols, the more efficient working with client dropouts, and the stronger protection of the advanced attacks. Also, the need to make sure that the secure aggregation designs are consistent with legal and regulatory provisions increases. These gaps will be of significance to deploy secure and legally-compliant machine learning systems in the real-world public health settings.

IV. FEDERATED LEARNING PRIVACY RISK

Despite the use of federated learning, there are still privacy hazards that are faced in various phases of training. The Figure 3 demonstrates the workflow of federated learning and outlines the main aspects at which privacy violations can be made. This is because the first model is distributed to an engineer and several users, where they are trained locally with personal data. The trained updates are sent to a central point computer to be federated. The lightning icons in the figure represent the possible privacy risk when transferring data, aggregation at the server side and the exposing of the model to the engineers. These dangers consist of updating interception, model parameter inference, and reconstruction of sensitive user data. The figure explicitly indicates that privacy leakage is not completely removed by federated learning despite the fact that raw data are still local and this is why the implementation of differential privacy mechanisms is necessary.

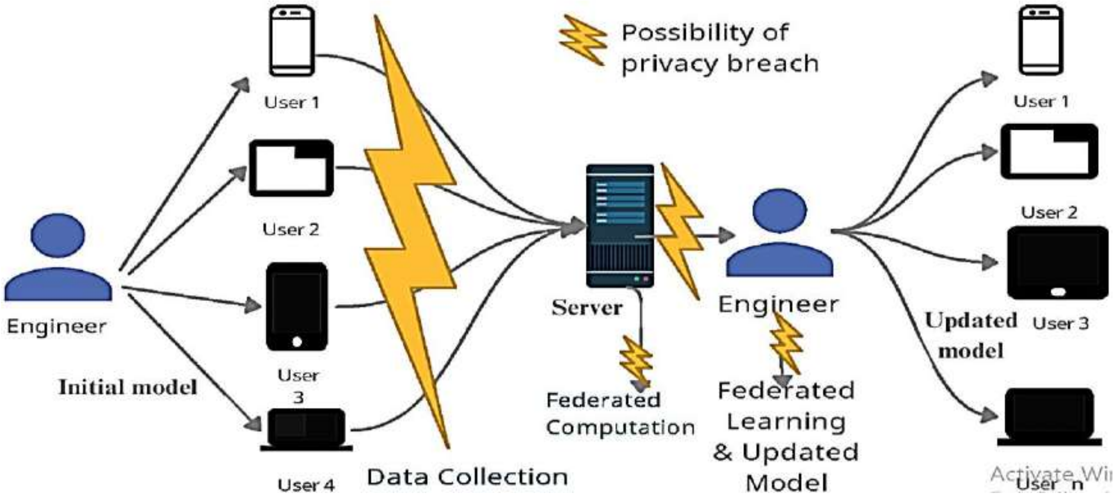


Figure 3: federated learning workflow

Privacy threats occur at different stages of the training process even in a federated learning case where such a learning is abused. As Figure 3 illustrates, the federated learning workflow presents the emphasis and highlights some of the locations where the privacy breaches might occur. The first model is transferred to a few users by an engineer, which trains the model locally on their own private data. The federated computation is performed through transmitting the trained updates to a central server. The figure has lighting indications which signify the potential risk of privacy, in case of data transmission, aggregation in the servers, and engineering access of models. Such risks are interception of updates, inference of model parameters, reconstruction of sensitive user data. It is evident in the figure that although raw data still remains local, federated learning alone does not completely avoid the leakage of privacy and thus warrants the adoption of differential privacy mechanisms.

During the data collection step, the users/institutions train models and send the update to a server in their local environment. Assuming that these updates are not properly secured and sent, attackers might intercept the communications or the attacker may use the patterns of updates to interpret them. This type of attack can reveal the characteristics of sensitivity, including details of disease condition or demographics.

This danger increases with an abundance of updates, or when the number of participants is limited.

The aggregation process itself is also a possible point of attack on a server level. An inquisitive server or an ill-intentioned employee working inside can attempt to peep into what is going in upgrades or compare one version of the models to another in order to deduce confidential information. Sensitive information can leak out even when using the system by engineers who are either managing the system or deploying it unless the privacy is tight.

Lastly, during the model distribution phase, the participants are supplied with the model updates. In case such models capture excessive information on individual sample data, attackers can execute membership inference attacks or model inversion attacks. Figure 3 identifies these weak spots and shows that federated learning is insufficient to make privacy threats a nonexistent problem.

A. The way Differential Privacy Remedies These Risks:

Differential privacy reduces such risks by limiting the contribution any given participant has on the final model. This is typically done by introducing noise to model updates prior to sharing or aggregating [24]. Therefore, whereas, an attacker can possibly access the updates or the models, the noise makes it very hard to obtain meaningful personal information.

Differential privacy may be implemented on various levels in federated learning systems. Local differential privacy: noise is introduced at the client side and then the updates are sent on the device - a very strong privacy property but poor model performance Central differential privacy: noise is added after the aggregation process which tends to be much more accurate but needs to trust the aggregation server. The systems will be able to receive a layered protection by integrating differential privacy and secure aggregation systems. Secure aggregation closely conceals the individual update and differential privacy does not allow any information to leak out even of the aggregated output. When combined, they provide more protection against external aggressors and internal threats.

B. Privacy-Accuracy Trade-offs and Practice:

One of the biggest issues of differential privacy is the privacy versus performance trade-off on the model. More aggressive privacy guarantees require additional noise, and this might lead to inaccurate model. The problem of low accuracy may affect the detection of outbreaks or resource plans in the infectious disease prediction, and thus, the tradeoff is significant. A careful choice of the privacy parameters must be made by researchers in order to attain the balance between protection and utility. Practically, this balance is founded on the practicality, sensitivity of the information and the degree of risk which can be taken. Small or highly imbalanced datasets can be more expensive to performance loss as well as large datasets can be relatively more noise-tolerant.

The difficulty of the systems is another challenge. Differential privacy must be implemented with a bit of care and professional skills [25]. Systems that are not properly configured can give an illusion of security or even breach privacy assurances. These issues highlight the significance of uniformity in guidelines and tools to use in the application of the differential privacy in the field of health.

C. Compliance to Law and Research Gaps:

Different privacy is significant towards meeting the legal and ethical demands of handling health information. A significant number of the data protection laws are aimed at minimizing data, anonymizing and risk reduction. Differential privacy directly promotes such principles by restricting the levels of exposure of the individual-level.

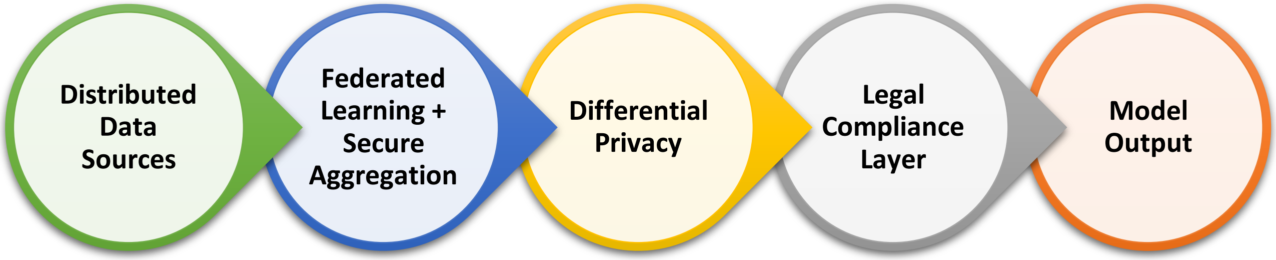
Although it has been strong, it has a number of research gaps. Further development is needed to obtain higher precision in the strict privacy budgets (especially detection of rare diseases). Little is also known concerning the manner in which privacy parameters that are legal can be selected. The adaptive privacy mechanism and improving the linkage between technical and regulatory complies should be a research topic in the future.

V. LEGAL AND ETHICAL COMPLIANCE

A major problem that can be raised in connection with the machine learning context is legal and ethical compliance that can be achieved when working with sensitive health or personal data [26]. A combination of federated learning with secure aggregation and differential privacy provides a feasible means of reducing risks associated with the failure to comply with privacy regulations including the General Data Protection Regulation (GDPR) in Europe, or the Health Insurance Portability and Accountability Act (HIPAA) in the United States [27]. It is possible to note that during the training of a model, the user data are stored on the local devices as indicated by the conceptual workflow in Figure 2 and Figure 3. Model updates as opposed to raw data are only shared with a central server. Secure aggregation ensures that, such updates are aggregated in a manner that the server or any external viewer would not be able to get access to the individual contributions. This process is directly connected with the idea of minimizing the data, which is one of the most important values of GDPR, as personal information is never revealed or concentrated at all. Differential privacy provides an additional level of compliance ensuring that compliance occurs by introducing noise on the model updates, which makes it mathematically challenging to learn anything about any individual [28]. These techniques combined reflect the principle of privacy-by-design, which proposes privacy protection to be implemented at the system architecture level, as opposed to being applied as an afterthought. Another way of promoting compliance is by adopting access controls and auditing systems and by making sure that only authorized individuals can work with model updates or aggregated outcomes. Through a federated learning method combined with secure aggregation and differential privacy, organizations will be able to demonstrate that they have made optimal efforts to make sure that sensitive information is secured, restricted, and compliant with the legal and ethical provisions of the major privacy frameworks. This combined effort reduces the possibility of incurring regulatory infractions, assists in ensuring that the operations are congruent with ethics so that gathering, storing and processing of valuable health data is carried out in a responsible manner. The conceptualized workflow shown in Figure 2 and Figure 3 shows the various levels of protection such that the data is stored locally, the communication is encrypted and the aggregation and redistribution would not be designed in a way to leak out. By doing so, the framework will be technically well-grounded and legally and ethically well-grounded, which will offer a practical plan of how secure and compliant machine learning can be in healthcare applications, in the real world.

VI. INTEGRATED FRAMEWORK

In order to establish privacy protection and still be legal, a combined system consisting of federated learning and secure aggregation and differential privacy can be implemented. The conceptualization of Figure 2 and Figure 4 explain how decentralized sources of data can be used to train a model without concentrating on sensitive information. The storage of raw data in this framework is done on the local device of each user and the computations are done locally. The updates are then transferred safely with the help of aggregation protocols, which do not permit the central server of knowing the individual contributions. The aggregated updates are done using differential privacy, as a form of additional obfuscation of the possibility of a leak of private data. The integrated process may be considered a layered architecture at the bottom, there are distributed data sources, which are inputs to the federated learning system with secure aggregation. The middle tier employs the concept of differential privacy on the aggregated model in such a way that the input of each participant in the data is mathematically safeguarded. Lastly, a layer of law-abiding presents a top-down method to the computation workflow and guarantees such ideas as privacy-by-design, data minimization, and adherence to regulations. With this architecture, the results of the model can be distributed to the researchers or decision-makers without compromising individual privacy. The framework also allows the ongoing learning and change as updates are made in a piece-meal manner and privacy-sensitive, which is highly important in areas like the medical field where data continuously change. In principle, then, this architecture means that the technical, legal and ethical concerns are closely fixed together. The distributed computation eliminates the threat of centralized attacks, an aggregation that defends against unauthorized access and during and the communication, and differential privacy eliminates the threat of inference attacks on the model itself. Law observance is enhanced through the paperwork of all the processes and evidence of the system in compliance to the norms of GDPR, HIPAA or other legal acts. This cumulative system provides a comprehensive privacy-conscious machine learning system: it enables joint model training, reduces exposure to sensitive data, and does not violate ethical and legal standards. The diagram below was used as a visual representation towards reinforcing the idea of each layer playing a role in ensuring privacy protection as well as regulatory compliance besides offering a clear and workable blueprint of what is needed to be implemented in the application of the concept in real-life application. When integrated within one system, organizations will be able to make sure that machine learning models are efficiently, securely, and responsibly trained



.

Figure 4: Integrated Workflow Diagram

VII. OPEN CHALLENGES & FUTURE DIRECTIONS

Federated learning (FL) is a new approach towards utilizing the information provided by different users without access to the raw data. Still, according to Figure 2 and Figure 3, there are still several privacy risks. Attackers can intercept or analyse updates sent by users to the server. It can be the server itself which can be attacked. The updated model can give sensitive information even during aggregation, depending on how weak the protection is. These weaknesses limit the use of FL to the real-life health applications.

Lightweight differential privacy (DP) is one of them. A significant number of customers use FL with their mobile devices. Mobiles have low calculating capabilities [29]. The existing DP techniques are bulky and slow and this reduces the rate of training. Studies are required to come up with DP that can effectively operate in mobile devices but safeguard privacy.

Attack resistant aggregation is another problem. Aggregation in this case (see Figure 2) takes place at the server. Assuming that attackers control part of the users or execute manipulative updates, they can cause bias on the end model. Attacks should be detected and prevented by new aggregation techniques; the model should be kept reliable and secure.

Also, a major goal is real-time outbreak detection. Figure 1 demonstrates that there is a great region-specific variation of infectious diseases. It is in dire need of the data collection and process in time to respond to outbreaks. The federated learning must be able to update faster and give early warnings, without violating privacy.

Other research directions include combining the idea of federated learning and secure computation, or combining adaptable machine learning models to the differences in the disease prevalence between regions. Confidentiality laws like GDPR also imply that one has to be careful when dealing with health information. More confidence will be developed in FL systems through the use of methods that comply with legal requirements and are effective. To conclude, Figure 2 and Figure 3 indicate that privacy violation and attacks may occur at various levels. The future studies should address these weak points and rectify them, and enhance efficiency of mobile and cloud systems, and generate dependable insights and real time to public health.

VIII. CONCLUSION

As presented in this review, on-hand infectious disease statistics, such as Figure 1, indicate the necessity to conduct massive health surveillance. The effects of the disease transmission of covid-19, dengue, and other infectious diseases vary in various regions. A collection of data in communities is an essential procedure but has privacy risks. Federated learning is a model training methodology that does not involve the exchange of the raw data. Figure 2 and

Figure 3 demonstrate the functioning of FL and the points of privacy risks. Aggregation is safely made to ensure that separate updates are safely put together. Differential privacy limits the contribution made by each user and limits inference attacks. The combination of the techniques allows securing technical and legal standards to manage sensitive health information.

The gaps and challenges are also determined in the review. The mobile applications need lightweight different privacy. Methods of aggregation must also withstand attacks and systems must have the ability to identify the outbreaks in real time. FL also needs to respond to variations in the prevalence of diseases across regions as indicated in Figure 1. To sum up, privacy-preserving machine learning is significant to the public health use. Figure 1, Figure 2, Figure 3 provide us with a reasonable notion of the actual world motivation, workflow of federated learning and potential privacy threats. The combination of both secure aggregation and differential privacy addresses the majority of these issues. The future research area would be to increase efficiency, privacy versus attacks, and patterns of disease in the region. This will enable effective, quick and secure monitoring of the population health to enable community to react to the threat of infectious diseases without compromising privacy.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] Q. Liu *et al.*, “Global distribution and health impact of infectious disease outbreaks, 1996–2023: A worldwide retrospective analysis of World Health Organization emergency event reports,” *Journal of Global Health*, vol. 15, Art. no. 04151, May 2025. Available from: https://doi.org/10.7189/jogh.15.04151

[2] R. Nasim, J. F. Tisha, and Syed, “Only COVID-19 and not all infectious diseases are of concern: A timely observation,” *Health Science Reports*, vol. 6, no. 9, Sep. 2023. Available from: https://doi.org/10.1002/hsr2.1589

[3] A. D. Pinto *et al.*, “Machine learning applications in population and public health: Guidelines for development, testing, and implementation,” *JMIR Public Health and Surveillance*, vol. 11, Art. no. e68952, Oct. 2025. Available from: https://doi.org/10.2196/68952

[4] A. Rahman *et al.*, “Machine learning and deep learning-based approach in smart healthcare: Recent advances, applications, challenges and opportunities,” *AIMS Public Health*, vol. 11, no. 1, pp. 58–109, Jan. 2024. Available from: https://doi.org/10.3934/publichealth.2024004

[5] A. Shahid, T.-A. N. Nguyen, and M.-T. Kechadi, “Big data warehouse for healthcare-sensitive data applications,” *Sensors*, vol. 21, no. 7, Art. no. 2353, Mar. 2021. Available from: https://doi.org/10.3390/s21072353

[6] A. K. Conduah, S. Ofoe, and D. Siaw-Marfo, “Data privacy in healthcare: Global challenges and solutions,” *Digital Health*, vol. 11, Art. no. 20552076251343959, May 2025. Available from: https://doi.org/10.1177/20552076251343959

[7] B. Yurdem, M. Kuzlu, M. K. Gullu, F. O. Catak, and M. Tabassum, “Federated learning: Overview, strategies, applications, tools and future directions,” *Heliyon*, vol. 10, no. 19, Art. no. e38137, Sep. 2024. Available from: https://doi.org/10.1016/j.heliyon.2024.e38137

[8] C. O. Idahor *et al.*, “Infectious disease surveillance in the era of big data and AI: Opportunities and pitfalls,” *Cureus*, Oct. 2025. Available from: https://doi.org/10.7759/cureus.93929

[9] P. J. Assudani *et al.*, “Artificial intelligence and machine learning in infectious disease diagnostics: A comprehensive review of applications, challenges, and future directions,” *Microchemical Journal*, vol. 218, Art. no. 115802, Oct. 2025. Available from: https://doi.org/10.1016/j.microc.2025.115802

[10] A. H. Seh *et al.*, “Healthcare data breaches: Insights and implications,” *Healthcare*, vol. 8, no. 2, pp. 1–18, 2020. Available from: https://doi.org/10.3390/healthcare8020133

[11] I. Siniosoglou *et al.*, “Federated learning models in decentralized critical infrastructure,” in *River Publishers eBooks*, pp. 95–115, Nov. 2023. Available from: https://doi.org/10.1201/9781032632407-7

[12] S. M. Narayan, N. Kohli, and M. M. Martin, “Addressing contemporary threats in anonymised healthcare data using privacy engineering,” *npj Digital Medicine*, vol. 8, no. 1, Mar. 2025. Available from: https://doi.org/10.1038/s41746-025-01520-6

[13] W. Yang *et al.*, “Deep learning model inversion attacks and defenses: A comprehensive survey,” *Artificial Intelligence Review*, vol. 58, no. 8, May 2025. Available from: https://doi.org/10.1007/s10462-025-11248-0

[14] S. Mohammadi, A. Balador, S. Sinaei, and F. Flammini, “Balancing privacy and performance in federated learning: A systematic literature review on methods and metrics,” *Journal of Parallel and Distributed Computing*, vol. 192, Art. no. 104918, May 2024. Available from: https://doi.org/10.1016/j.jpdc.2024.104918

[15] I. Namatevs, K. Sudars, A. Nikulins, and K. Ozols, “Privacy auditing in differential private machine learning: The current trends,” *Applied Sciences*, vol. 15, no. 2, Art. no. 647, Jan. 2025. Available from: https://doi.org/10.3390/app15020647

[16] K. Hu *et al.*, “An overview of implementing security and privacy in federated learning,” *Artificial Intelligence Review*, vol. 57, no. 8, Jul. 2024. Available from: https://doi.org/10.1007/s10462-024-10846-8

[17] X. Zhang, Y. Luo, and T. Li, “A review of research on secure aggregation for federated learning,” *Future Internet*, vol. 17, no. 7, Art. no. 308, Jul. 2025. Available from: https://doi.org/10.3390/fi17070308

[18] F. J. Piran, Z. Chen, M. Imani, and F. Imani, “Privacy-preserving federated learning with differentially private hyperdimensional computing,” *Computers and Electrical Engineering*, vol. 123, Art. no. 110261, Mar. 2025. Available from: https://doi.org/10.1016/j.compeleceng.2025.110261

[19] A. Blanco-Justicia *et al.*, “Achieving security and privacy in federated learning systems: Survey, research challenges and future directions,” *Engineering Applications of Artificial Intelligence*, vol. 106, Art. no. 104468, Nov. 2021. Available from: https://doi.org/10.1016/j.engappai.2021.104468

[20] K. Kalodanis *et al.*, “A privacy-preserving and attack-aware AI approach for high-risk healthcare systems under the EU AI Act,” *Electronics*, vol. 14, no. 7, Art. no. 1385, Mar. 2025. Available from: https://doi.org/10.3390/electronics14071385

[21] T. Liu *et al.*, “High-accuracy low-cost privacy-preserving federated learning in IoT systems via adaptive perturbation,” *Journal of Information Security and Applications*, vol. 70, Art. no. 103309, Nov. 2022. Available from: https://doi.org/10.1016/j.jisa.2022.103309

[22] A. Ali, V. Snášel, and J. Platoš, “Health-FedNet: A privacy-preserving federated learning framework for scalable and secure healthcare analytics,” *Results in Engineering*, vol. 27, Art. no. 106484, Sep. 2025. Available from: https://doi.org/10.1016/j.rineng.2025.106484

[23] A. Adnan *et al.*, “A secure and privacy-preserving approach to healthcare data collaboration,” *Symmetry*, vol. 17, no. 7, Art. no. 1139, Jul. 2025. Available from: https://doi.org/10.3390/sym17071139

[24] Y. Wang *et al.*, “Differential privacy in deep learning: Privacy and beyond,” *Future Generation Computer Systems*, vol. 148, pp. 408–424, Nov. 2023. Available from: https://doi.org/10.1016/j.future.2023.06.010

[25] N. Lefkovitz, *Guidelines for Evaluating Differential Privacy Guarantees*, NIST Special Publication 800-226, Oct. 2024. Available from: https://doi.org/10.6028/nist.sp.800-226

[26] T. Pham, “Ethical and legal considerations in healthcare AI: Innovation and policy for safe and fair use,” *Royal Society Open Science*, vol. 12, no. 5, May 2025. Available from: https://doi.org/10.1098/rsos.241873

[27] A. Horst *et al.*, “Federated learning: A privacy-preserving approach to data-centric regulatory cooperation,” *Frontiers in Drug Safety and Regulation*, vol. 5, May 2025. Available from: https://doi.org/10.3389/fdsfr.2025.1579922

[28] H. K. Tayyeh and A. Sabah, “Balancing privacy and performance: A differential privacy approach in federated learning,” *Computers*, vol. 13, no. 11, Art. no. 277, Oct. 2024. Available from: https://doi.org/10.3390/computers13110277

[29] S. Guo *et al.*, “Federated learning with differential privacy via fast Fourier transform for tighter-efficient combining,” *Scientific Reports*, vol. 14, no. 1, Nov. 2024. Available from: https://doi.org/10.1038/s41598-024-77428-0