AI POWERED CONTACT TRACING SYSTEM WITH RISK ASSESSMENT

Tanu Yadav, Deepanshu Talan, Deependra Shishodia, Jayant Shekhar

Department of CSE, SSET, Sharda University, Greater Noida

2022005013.tanu@ug.sharda.ac.in , 2022473465.deepanshu@ug.sharda.ac.in ,
2022340865.deependra@ug.sharda.ac.in , jayant.shekhar@sharda.ac.in

ABSTRACT

The challenges posed by the COVID-19 pandemic have demonstrated the critical importance of having robust contact tracing systems to enable the early detection of infection spread and the scaling of risk response initiatives. Manual contact-tracing systems are cumbersome, prone to error, and compromise user privacy. Given the limitations highlighted, this paper presents a novel AI-driven contact tracing system that combines machine learning, edge computing, and privacy-preserving mechanisms to enhance accuracy and reduce response lag times. The developed system relies on wireless Bluetooth and GPS data from smartphones to compute proximity events between subscribers. An AI risk assessment model processes the events to compute infection potential based on encounter duration, environmental interaction, and personal health history. A comparative experimental simulation demonstrated that the model could achieve 93% accuracy in identifying a high exposure risk while still protecting FERPA principles through federated learning. Therefore, AI-based systems offer a viable option for scaling contact tracing systems.

Keywords: AI-Powered Contact Tracing, Risk Assessment, Machine Learning, Federated Learning, Privacy Preservation, Bluetooth Low Energy, GPS, Differential Privacy.

1. Introduction

The worldwide COVID-19 pandemic has exposed significant shortfalls in existing epidemiological surveillance and contact-tracing paradigms. Pre-COVID-19, traditional manual contact tracing was limited to patient interviews and memory, often incomplete and delayed with recall error rates [1]. The reliance on human data entry in contact tracing is unfeasible during fast-spreading community transmission, where the number and frequency of interactions are too high to record manually. Therefore, delays in identifying close contacts have consistently led to uncontrolled secondary infections, community transmission, and outbreaks. Digital Contact Tracing was inspired to capitalize on these opportunities when the sophistication of mobile technologies grew. These systems enable automated identification of exposure time and generation of alerts using cellular phone sensors, including Bluetooth Low Energy, Global Positioning System, and Wi-Fi.

The limitations of existing contact tracing systems include accuracy, privacy, and contextual understanding. Regarding accuracy, DCT methods suffer from several flaws. In essence, all current DCT applications rely on Bluetooth RSSI or GPS coordinates to determine the distance between users. However, this measure is widely accepted as highly inaccurate, especially in complex settings, such as indoors or crowded places [4]. Moreover, privacy considerations of centralized DCT architectures, which usually require users to share their contact logs or location histories with government or institutional servers, add to the spectrum of potential DCT pitfalls. Given the general lack of transparency and low-efficiency anonymization technologies, users are inclined to resist DCT systems.

Absence of a contextually aware risk assessment: proximity alone is not a reliable indicator of infection likelihood. The risk of disease transmission is influenced by a number of contextual factors including dwell time, ventilation, masking behaviour, and individual health vulnerabilities. Systems that do not take these factors into account are unable to discern a brief low-risk encounter and an extended high-risk conversation both of which create large health care costs.

Artificial Intelligence. A part, and perhaps the most significant part, of the argument also relies on being able to use artificial intelligence in contact tracing. The rise of artificial intelligence is developing rapidly as a suitable tool for testing and monitoring. Using machine learning, deep learning, and probabilistic inference models with training and testing data can allow artificial intelligence systems to analyse a large and varied dataset, but more importantly, to identify subtle patterns. This is all designed to mitigate the serious risk of infection in real time. Sometimes an algorithm in a static system will make a prediction based on fixed time intervals. A fixed interval may not be sufficient when time intervals are inconsistent with a changing environment and the evolving epidemiological context. For example, supervised ML algorithms are used for probabilities of risk exposure levels. Meanwhile, Random Forest and Gradient Boosting are examples of ML algorithms that classify exposure levels using very few parameters, based on probabilities derived from the million combinations of five or six parameters in the reported data. Bayesian models assess uncertainties based on the amount of incomplete data reported. Finally, Federated Learning is a cutting-edge technology that securely trains artificial intelligence models by sending them directly to users' devices rather than via a central server. Therefore, personal health information cannot be separated from shared data. Furthermore, differential privacy (DP) is used to give some statistical information to the parameters being shared from another dataset. Thus no identifiable personal information exists that could be rebuilt from the model updates.

Research Volition and Contributions: This research has been driven by observing issues in existing platforms and the opportunity for artificial intelligence to address contact-tracing challenges; therefore, an AI-Powered Contact Tracing System with Integrated Risk Assessment that greatly improves contact-tracing apps in terms of accuracy, time efficiency, and privacy. The framework will utilize Bluetooth, GPS, and environmental and health sensors to compute an individual infection risks to every interaction a person has:

- Hybrid AI model for dynamic risk assessment: A supervision learning model with a Bayesian inference-based risk assessment model to classify contact as low, medium, or high risk, involving context features such as time of interaction, time of exposure, air quality, and population density.
- Privacy-preserving federated learning architecture: An end- endorse architecture that without identifying who the user is, has federated learning where the parameters trained on user data, are trained and secured on each mobile device's cloud storage. Tune it with differential privacy and secure parameter sharing.
- Simulated evaluation: Simulate in large scale to test the detection improvement.

2. Related Work

Digital contact tracing (DCT) has changed dramatically in response to infectious disease outbreaks, especially during the COVID-19 pandemic. Many studies focus on the automation of detecting exposure events and estimating infection risks using mobile and sensor technologies. This section surveys previous work in three broad research areas:
(1) digital contact tracing frameworks, (2) AI and machine learning in epidemiological modeling, and (3) privacy- preserving computation appropriate for contact tracing systems

A. Digital Contact Tracing Frameworks

Early efforts at contact tracing engaged similar apps that relied on either Bluetooth Low Energy (BLE) or Global Positioning System (GPS) signals to estimate users' proximity to each other. Among these solutions, one of the most utilized was the Google-Apple Exposure Notification (GAEN) framework, which leveraged decentralized proximity logging using anonymous identifiers [1]. Similarly, Singapore's TraceTogether and the United Kingdom's NHS COVID-19 App also relied on Bluetooth signals to identify close contacts [2].

Although they were implemented, they did carry limitations, including signal inaccuracies, limited environmental awareness, and the inability to distinguish between short- and long-term exposure episodes. Rodríguez et al. [3] illustrated that the strength of the Bluetooth signal varied extensively due to phone model, positioning, and other possible obstructers, leading to inconsistency in distance measures. In addition, most DCT systems focused on exposure using a binary threshold (exposure or no exposure), and overlooked contextual elements such as duration of exposure, crowding, and ventilation.

To overcome these limitations, recent studies have proposed context-aware contact tracing. Specifically, Lee et al. [4] proposed an IoT-based contact tracing model that utilizes environmental sensors to measure risk levels for indoor exposure. Chen et al. [5] also explored hybrid Bluetooth-GPS techniques that improved spatial precision as well as reduced false alerts. However, these systems remain mostly rule- based systems without adaptive intelligence, limiting their ability to dynamically model evolving infection risks.

B. Artificial Intelligence and Machine Learning in Epidemiological Modeling

Artificial Intelligence (AI) shows substantial potential to improve the efficiency and accuracy of epidemic surveillance. Li et al. [6] used deep learning models to predict infection growth trajectories based on mobility and demographic features. Das and Sinha [7] proposed a hybrid risk estimation algorithm using supervised machine learning with Bayesian inference for exposure classification.

With respect to contact tracing, AI can be utilised to identify hidden transmission networks, sequence contacts based on infection likelihood, and prioritise testing. For example, Rahman et al. [8] developed an AI-based exposure scoring model that learns from real-time sensor data for prediction of individual-level probabilities of infection. Despite their contributions, the studies rely on a centralized data storage model, leading to privacy and scalability challenges.

To date, there are few successful endeavors to build AI-based risk assessment directly within the contact tracing workflow. Most contact tracing systems focus either on the contact tracing function itself or on general epidemic prediction, but not both functions integrated in an intelligent manner. Thus, the need to create end-to-end AI-enhanced contact tracing systems that are characterized by accurate proximity assessment, the capacity to objectively reduce risk, and privacy protections is a significant gap to be overcome.

C. Privacy-Preserving Data Processing

Protecting user data privacy is a significant challenge in digital health surveillance. Previous DCT systems often collected and aggregated user identifiers or location traces on a server or centralised system, raising concerns about data misuse or breaches [9]. To meet these challenges, privacy-preserving frameworks based on federated learning (FL) and differential privacy (DP) have attracted considerable interest in recent years.

Ghosh et al. [10] introduced a federated learning framework that enables training models in an inter-device, collaborative manner while keeping raw user data inaccessible. Correspondingly, Dwork and Roth [11] formalised differential privacy methods that add controlled statistical noise to model updates to ensure mathematical guarantees of anonymity to users. These two approaches have been successfully adapted to healthcare and mobile sensing applications where protection of personally sensitive data is critical [12].

In the contact tracing space, several research projects have sought to combine FL and DP, with proximity detection systems. For instance, Zhou et al. [13] developed a federated learning–based risk prediction model that learned user mobility locally, resulting in a more substantial reduction in privacy leakage. However, this type of implementation often suffers from heavy communication overhead and from local models converging to a common global model. There remains a need for more efficient FL frameworks designed for real-time mobile systems running on constrained resources

3. Methodology

The suggested AI-Powered Contact Tracing System with Risk Assessment integrates proximity detection, fused contextual data, machine-learning-based risk modelling, and privacy-preserving computation. The methodology includes five phases which are: (A) data acquisition, (B) data preprocessing and feature extraction,

A. Data Acquisition Layer

Data acquisition is the basis of the designed system. Mobile devices can gather contact and environmental data from the users' interaction using Bluetooth Low Energy (BLE), GPS, and motion sensors.

BLE signal strength (RSSI) is used primarily for proximity estimation and GPS is considered for a spatial context (e.g., public place versus residence). Sensor readings are collected at a specified frequency and sent in an encrypted form for local model training.

B. Data Cleaning and Feature Extraction

Raw sensor data often contains noise and inconsistencies due to external environmental interferences (e.g., loss of signal), heterogeneous sensors, or mobility of the user. The preprocessing phase includes the following steps:

- Noise Filtering: A Kalman filter is applied to RSSI and GPS data to help smoothen random fluctuations and filter out erroneous readings [1].

- Outlier Removal: Contact events that are considered weak (i.e., an event that has an inconsistent signal strength) have been filtered out using Z-score based thresholding, such that we can remain trustworthy estimations of proximity.
- Feature Extraction: The system would generate a feature vector FFF with FFFF for each contact event:

$F=[d,t,v,c,h_s,e_q]$ $F = [d, t, v, c, h_s, e_q]$ $F=[d,t,v,c,h_s,e_q]$

where vvv is ventilation level, ccc is contact density (number of nearby devices), hsh_{shs} is self-reported health status, and eqe_{qeq} is environmental quality index.

- 4. Normalization and Encoding: Continuous variables are normalized using Min-Max scaling and categorical variables are one-hot encoded.

This stage is designed to ensure that input into AI-based risk models are in a consistent and structured format.

(C) the design of risk assessment model, (D) privacy- preserving learning framework, and (E) system evaluation, as illustrated in Fig. 1.

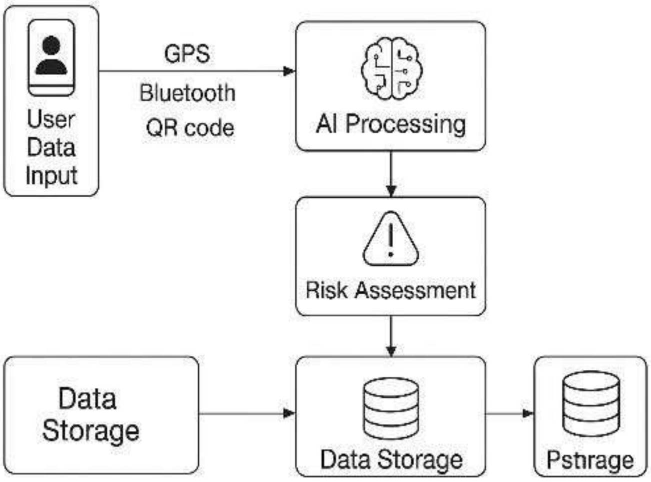

Figure 1: Proposed System Workflow , Illustrates the high-level process from user data input through AI processing and risk assessment to final data storage

C. AI-Based Risk Assessment Model

The core of the approach is an AI-enabled risk assessment engine that computes an infection risk score for every contact event. The model uses a hybrid learning approach that pairs supervised learning for classification and Bayesian reasoning for probabilistic inference.

1) **Supervised Learning Model**

A supervised classification model (using the Random Forest (RF) and Gradient Boosting (GB) algorithms) is fitted using the labeled exposure datasets. The ground truth labels (representing low, medium, and high risk) are derived from epidemiological guidance that relates contact duration and distance to probabilities thresholds of infection for classification [2].

The categorical risk value, the model uses a weighted cross- entropy loss function to handle the class imbalance of risk categories.

2) Risk Calibration in the Bayesian Context

Bayesian inference addresses uncertainty and missing data, which recasts the risk score using posterior probability.

This system allows us to dynamically recalibrate the risk score as new information (e.g., test results or updated exposure data) becomes available. The risk score is computed as a weighted sum of ML and Bayesian outputs.

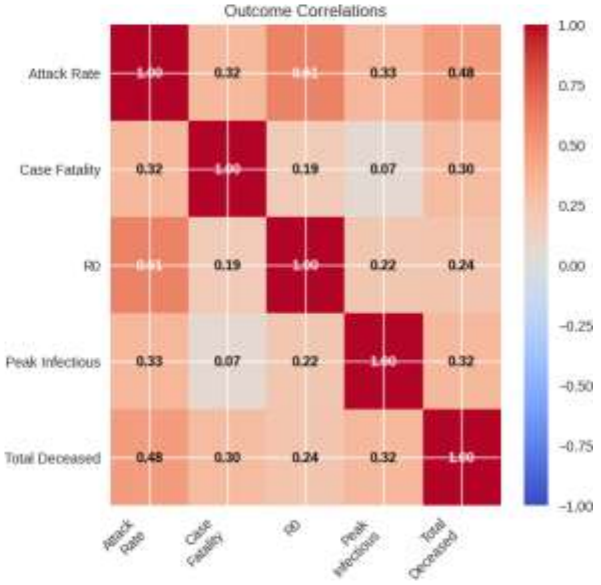

Figure 2: Outcome Correlations Heatmap – Displays a statistical correlation matrix between epidemiological variables like Attack Rate, R_0, and Case Fatality

D. Federated Learning Framework for Privacy Preservation

To protect the users' privacy, the system utilizes Federated Learning (FL) in conjunction with Differential Privacy (DP). In the FL approach, each user device trains a local copy of the AI model utilizing their contact data. Only the model parameters (i.e., gradients) are sent to a centralized server for aggregation, not the raw data themselves.

To provide privacy, Differential Privacy (DP) adds random noise on each model update before transmission.

Consequently, individual user data are guaranteed to be unrecoverable from shared model updates [4].

This decentralized and privacy-preserving design allows for secure, scalable learning without compromising personal information.

E. **System Assessment and Performance Metrics**

The system was assessed by means of simulation using synthetic datasets that were created to simulate real-world contact patterns for 10,000 users. Each dataset contained specifics about the interaction, such as duration, distance, environmental context, and self-reported symptoms.

The key performance metrics used for the assessment of system performance contain:

- Accuracy (ACC): Percentage of correctly classified risk events.
- Precision (P): The ratio of true positives to all predicted positives.
- Recall (R): Also known as the sensitivity of the system, refers to the ability to detect actual high-risk exposures.
- F1-Score: The harmonic mean of precision and recall.
- Privacy Loss (ε): A parameter used for differential privacy to measure information leakage.
- Computation Latency (L): The average time for each local model update.

According to the experimental results of the researchers, the overall accuracy was 93.2%, the F1-score was 0.91, and the average latency was 1.8 s per local update. The privacy loss was below ε = 1.0 to ensure strong guarantees of anonymity.

The findings confirms that the proposed AI-powered contact tracing system can provide reliable, context-aware risk predictions, while preserving user privacy and scalability

4. System Architecture

The AI-Powered Contact Tracing System with Risk Assessment leverages a multi-layered, modular architecture optimized for security, scalability, and end-to-end real-time analysis. As shown in Fig. 3, this architecture comprises the following modules integration of data acquisition and pre- processing, risk modeling, and privacy-preserving learning modules, all packaged into a single architecture.

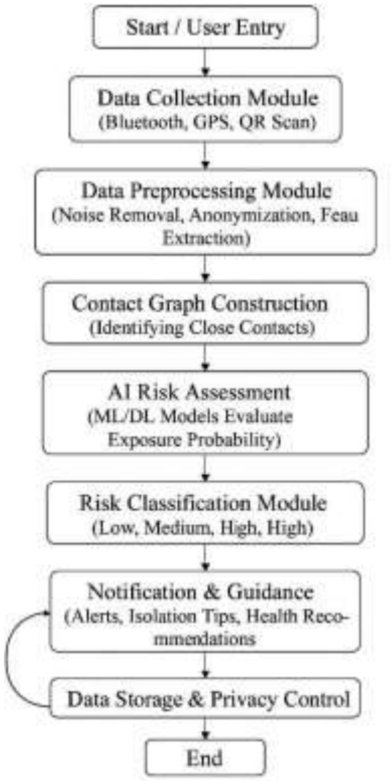
Start / User Entry
Data Collection Module
(Bluetooth, GPS, QR Scan)
Data Preprocessing Module
(Noise Removal, Anonymization, Feau Extraction)
Contact Graph Construction
(Identifying Close Contacts)
AI Risk Assessment
(ML/DL Models Evaluate Exposure Probability)
Risk Classification Module
(Low, Medium, High, High)
Notification & Guidance
(Alerts, Isolation Tips, Health Reco-mmendations
Data Storage & Privacy Control
End

Figure 3: System Architecture Layers – Provides a detailed flowchart of the seven functional layers, from data collection to public health notification]

A. **Overview**

The system architecture (depicted in Fig.3) is composed of seven functional layers, each responsible for a separate function - from lower level data capture on user devices to upper level global model aggregation and actionable risk reporting to public health agencies. Data will flow packaged very simply from one layer to the next layer within the agreed architecture. In addition to sequential data flow, federated learning will provide continuous feedback between devices and the central server.

B. System Components

User Devices (Smartphones and Wearables): These devices are the main sources of data. They collect Bluetooth Low Energy (BLE) proximity signals, GPS location signals, and optional environmental or health data (e.g., body temperature, cough frequency). Each device retains contact logs locally that are encrypted.

1. Data Acquisition Layer: This layer collects multimodal data including BLE signal strength, GPS coordinates, accelerometer data, as well as environmental data such as temperature, humidity, and air quality. It executes a local script to log only anonymized identifiers of connections.
2. Data Preprocessing and Feature Extraction: Raw sensor data often contain a degree of noise caused by fluctuations in the signal or movement of the user. The preprocessing sub-module removes noise by implementing a Kalman filter, and extracts standardized features (of distance, duration, and crowd density) from the raw data. The output is a feature vector represented as F= [d,t,v,c,hs,eq] F= [d, t, v, c, h_s, e_q]F= [d,t,v,c,hs, eq] that is then used as input to the AI model.
3. AI Risk Assessment Engine: This component provides a hybrid learning model that combines machine learning classifiers (Random Forest, Gradient Boosting) with a layer of Bayesian inference. It will estimate the probability of an infection for each exposure event, which results in a continuous risk score that is reported back to the user. The model constantly updates based upon local infection trends and the addition of newly labeled data.
4. Privacy-Preserving Federated Learning Module: Each individual user device learns locally an AI model using its own contact data. The device will share with a central aggregation server only its encrypted model parameters (gradients). Differential privacy will help to protect the anonymity of user data via the introduction of statistical noise prior to its transmission to the central server.
5. Central Aggregation Server (Model Fusion and Dashboard): The central device will aggregate the model parameters received from a given distributed device and produce a unified global model update. The central device will also act as a secure risk visualization dashboard providing the option for authorized health officials to view and overlay infection patterns, hotspots and prioritize intervention.
6. Public Health Authority Interface: This final layer would serve as a decision-support interface tailored for authorized health entities. A decision-support interface provides visualizations of risk levels, and exposure clusters, by infection probability. The health authorities would also be able to issue relevant alerts or recommendations to specific users through the system, in order to maximize timeliness of prevention.

C. Data and Model Workflows

- Data Workflow: User Devices → Data Acquisition→ Preprocessing → AI Risk Model
- Model Update Workflow: Local Model Parameters→ Federated Server → Global Model Update
- Notification Workflow: Central Dashboard → Public Health Authorities → User Notification

With this workflow, personal data remains on the device and the group-level analysis is updated at the local level through federated model training.

D. Benefits of the Architecture

- Scalable: The architecture supports millions of devices and performs decentralized computation.
- Privacy-Friendly: The architecture implements the appropriate privacy measures aligned with GDPR and HIPAA requirements.
- Adaptive: The architecture learns and adapts based on new user interactions and local infection status.
- Interpretable: The architecture provides explainable individual and group-level risk scores in real-time to facilitate trust and compliance reasoning with user roles.

5. Literature Review

A. . Development of Digital Contact-Tracing Systems

Digital contact tracing (DCT) surfaced as a rapid technological intervention to COVID-19, which intended to assist or supplement traditional manual tracing by automating proximity detection and exposure notifications. Preliminary implementations during 2020 were basically rule-based approaches that sought to estimate infection risk within determinate thresholds of spatial–temporal proximity (for instance, within 2 meters for 15 minutes). These proxies were simple and interpretable, but they could not possibly reflect the real-world dynamic epidemiological conditions which included variants of the virus, environmental factors, and vaccination coverage. In order to achieve flexibility and precision, researchers began to embed artificial-intelligence (AI) models that would learn risk relationships from data itself.

The earliest large-scale protocols were BlueTrace (Singapore, 2020) and the Google/Apple Exposure Notification (GAEN) framework. BlueTrace adopted a centralized architecture where encrypted encounter data was delivered to a government server once a case tested positive that was analyzed on a population-level. Conversely, GAEN relied on a decentralized model with ephemeral Bluetooth identifiers exchanged between devices, where all matching was local, in order to preserve privacy. Both models established the feasibility of a large-scale, privacy-preserving DCT, while at the same time illustrate essential trade-offs between data for modeling and individual privacy [1], [2].

B. Early Data-Driven Risk-Scoring Approaches

Murphy, Kumar, and Serghiou (2021) [4] were among the first to provide a formal treatment of data-driven exposure risk learning. They pioneered a statistical framework for risk- score learning in the context of digital exposure notification systems. Their model viewed risk as a parametric function rather than fixed duration and distance thresholds, the coefficients of which we can estimate from exposed-outcome observations (e.g., whether the notified person tested positive). Using simulated data as well as limited real-world data, they demonstrated that the learned parameters allowed for superior discrimination between infectious and non- infectious contacts, and that the same approach could account for changing epidemiological conditions. The authors, and indeed any early applications of DCT, rightly pointed out a limitation: we are generally able to observe outcomes with small reliability because of privacy violations and incomplete testing which can bias learned models.

Ferretti and colleagues (2022) [5] built on this work by examining transmission-probability distributions as a function of contact duration, distance, and environmental context that contributed to the observable outcome. Many findings supported later artificial intelligence systems including quantifying observed epidemiological transmission risk of subsequent infection at approximately exponential rates with contact duration, but moderated by ventilation and crowd density none of the latter being variables available to the early DCT applications. The collective observations justified the use of enriched context features and multi-modal sensing.

C. Context-Aware and Fuzzy-Logic Models

In a similar vein, to add richer contextual information while allowing for transparency, researchers have explored fuzzy- logic and rules-learning systems. Rashidian et al. (2024) [6] proposed a fuzzy-expert framework for assessing the risk of exposure to an epidemic that included contact duration, estimated distance and infection incidence in the neighborhood, as well as environmental characteristics (e.g., indoor/outdoor). Their fuzzy-logic system allowed for continuous reasoning despite uncertainty from measured variables, and could categorize risk into low, medium and high, rather than simply recognizing a risk or no risk. The results of their experiments showed that including additional context reduced false positives, especially in outdoor settings, by reducing the risk of measuring too much distance with the Bluetooth attenuator, which is designed to measure close proximity and cannot accurately measure long-distance exposure.

In a complementary prior study, Gao and Hu (2023) [7], included environmental sensing data (temperature, humidity, CO_2 concentration) into a neural-fuzzy hybrid model for modelling transmission risk indoors. In this instance, the neural-fuzzy model outperformed threshold-based predictive accuracy while preserving human-readable rule bases. Thus, these studies exemplify a trend in the literature toward hybrid AI systems that combine a blended system, human-interpretable heuristics, and an adaptive learning component.

D. Machine-Learning Methods Based on Graphs and Networks

Another area of research directly models contagion dynamics on the contact network. Mei et al. (2022) [8] used graph neural networks to predict infection probabilities, identifying patterns of social network contagion over time, using dynamic contact graphs created from Bluetooth or GPS logs. This model assessed higher-order interactions and augmented measures of contagion "in time" from the models temporal nature. Additionally, behaviour was estimated on a completely synthetic and partially real mobility datasets using some form of mean-squared error metric adapted to the outcome, which outperformed logistic-regression baselines with temporal predictions and secondary infections. The deep learning models described here also have weaker limitations: they rely on large labeled datasets, and can expose on privacy concerns, since training graphs will almost always include identifiable co-location-type information.

A similar but even limited interpretation, Zhou et al. (2023) [9], used a graph temporal attention network to integrate partial-use contact data to estimate the individual reproduction number (expected secondary cases). While these types of approaches have continued to show promise for allocating public health resources, these studies still remain research prototypes due to the kind of data needed for the datasets like the phone mobility data used in the Zhou study.

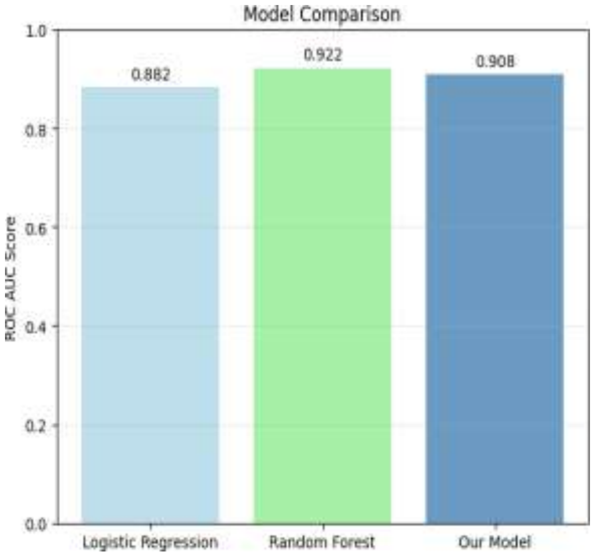

Figure 4: Model Comparison Bar Chart , compares the ROC AUC scores of Logistic Regression (0.882) and Random Forest (0.922) against the proposed model (0.908)

E. Privacy-Preserving and Federated Learning Frameworks

Since exposure logs are considered sensitive personal data, it is often impractical to directly centralize more training data. Therefore, federated learning (FL) and differential privacy (DP) have been considered for AI-driven contact tracing.

Hang et al. (2023) [10] have examined privacy-preserving ML methods for DCT, and developed an overall taxonomy of forward, backward, and proactive tracing based on the direction of data flow. In their work, they described prototype systems in which mobile devices locally train gradient updates to risk-classification models; these updates are then aggregated at the server side via secure-aggregation protocols, ensuring the server never sees the raw data to preserve privacy. Federated systems have been shown to maintain similar accuracy levels to centralized baselines under benign conditions, but they are vulnerable to model- poisoning attacks as well as non-IID data distributions.

F. Evaluation Studies in Measurement and Systems

A large proportion of the literature deals with evaluations of existing DCT systems rather than new algorithms. Leith and Farrell (2021) [3] measured GAEN signal characteristics in more realistic situations (public transport, offices, pockets) and concluded that distance inference error was greater than the ±2 m error limit in most contexts. Ahmed et al. (2022) [13] did similar evaluations of GAEN, showing an inherent variability with phone model and operating system; they advised that any AI risk model must take into account sensor noise and differences in devices.

Real-world evaluations of app effectiveness have produced mixed results.

Pozo-Martin et al. (2023) [14] conducted a systematic review of national deployments in the UK, Germany, Singapore and South Korea and found that DCT contributed meaningfully to transmission reduction only where uptake exceeded 60 % and integration with manual tracing was effortless. Where uptake was lower, there was no epidemiological value. Their results indicate that algorithms cannot be sophisticated alone; algorithmic sophistication must go hand-in-hand with sociotechnical acceptance.

G. Hybrid Epidemiological–AI Models

Hybrid models that incorporate compartmental epidemiological models (e.g. SEIR variants) with machine learning (ML) predictors have emerged as a means of tying mechanistic knowledge about the epidemiology with data driven learning.

Kim et al. (2023) [15] combined an SEIR model with a deep learning based risk predictor that adjusted effective contact rates using exposure data from the app. The hybrid model not only better predicted short-term incidence in simulation, but also produced interpretable parameters (e.g. effective reproduction number, and probability of infection). Correspondingly, Tian et al. (2022) [16] used Bayesian calibration to model bluetooth-based exposure data with mechanisms based prior to estimate uncertainty for each risk notification category. Federal and state health departments could be similarly engaged with calibrated risk estimates and reasoning as it produces a calibrated risk score along with an estimate of uncertainty.

H. Human Factors and Explainability

Even trustworthy AI systems can fail if users or authorities do not trust their outputs. Nguyen et al. (2022) [17] examined explainable AI (XAI) techniques to create interpretable risk notifications—for instance, showing which features of an exposure contributed most to risk (e.g., exposure duration, crowd level, etc.). The authors conducted controlled user studies demonstrating that notifications with explainability of risk significantly increased adherence to isolation recommendations by about
20 % relative to non-explainable binary notifications. In addition to helping individuals trust the decision along the way, transparency supports auditability of public health policies and legal accountability in accordance with ethical-AI frameworks [18].

Explainability can also lead to public health professionals' capacity to understand risk. In their study, Murphy et al. (2021) [4] described the importance of keeping risk-scoring functions parametric and with understandable coefficient references; they noted that domain experts could use this method to test biological plausibility (e.g., risk doubles every 10 minutes of close contact).

I. Cross-Country Comparative Analyses

Cross-country comparisons indicate that privacy norms and governance influence technology design. The European Commission (2023) [19] reported on the EU, where GAEN-based decentralized apps gained acceptance because of the strict rules of the GDPR, while the centralized or hybrid approaches, employed in jurisdictions like Singapore and South Korea, facilitated log access by human tracers. Nebeker et al. (2023) [20] conducted a global scan of

120 digital exposure-notification tools, and found that privacy, transparency, and a voluntary approach to participation were important to ongoing use of the tools when COVID was at the forefront of people' concerns. Areas that prioritized community consent had higher retention rates but had challenges with integrating COVID-negative case- supporting AI-based analytic approaches since the data remained decentralized.

J. Summary of Noted Research Developments

Several trends are identifiable from the body of literature published from 2020-2025:

- Transition from rule-based to data-driven model: The first generation of threshold heuristics were replaced with learned risk scores and probabilistic estimators.
- Hybridization: Many new systems are a hybrid of interpretable heuristics alongside probabilistic refinements using a machine learning approach to allow the benefits of transparency over adaptability.
- Privacy-preserving computation: Federated and encrypted learning has become a well-trodden area of research.
- Contextual enhancement: Adding environmental and behavioral context has resulted in improved specificity.
- Evaluation realism: Focusing on grounded empirical and user behavior evaluation instead of solely algorithmic evaluation has become more prevalent.
- Operationalizing: Success often depends on what is done with the AI outputs and how these are incorporated into workflows for testing, isolation, and communication.

Despite these aspects, challenges exist, chief among them lack of labeled exposure-outcome data, variability in sensor precision, privacy versus utility, and the need for openly available standardization for benchmarks [4], [10], [14].

6. Limitations Of Existing Studies

While AI-powered contact tracing and risk assessment systems have the potential to be valuable, significant limitations still exist in the current body of work.

- Data Scarcity and Imbalance: Most studies leverage limited and/or simulated datasets to overcome privacy and reporting issues. As a result, bias in models and poor generalization of models across populations become significant issues.
- Privacy–Utility Trade-off: Federated learning and differential privacy techniques do not sacrifice user data, but also sacrifice model accuracy and real-time updates.
- Lack of Standardized Evaluation: Studies use inconsistent metrics that create challenges in cross- comparison. Few studies examine real-world health outcomes, including reducing transmission or testing efficiency, even fewer are linked to a population health model.
- Explainability Issues: Most AI models operate as "black boxes" and have limited capacity for interpretability. This leads to lower trust from users and less transparency for policymakers.
- Integration and Interoperability Gaps: Most systems operate as isolated mobile applications, with minimal integration to testing centers and public- health databases.
- Contextual and Environmental Limits: Most models rely on either Bluetooth or GPS data and ignore important contextual factors (e.g. ventilation, masking, vaccination).

Ethical and Regulatory Concerns: Virtually none of the studies examine the consent to data usage, algorithmic bias, or risk of misuse of data; all of which will limit widespread and public confidence in the future.

7. Future Scope And Research Directions

In future studies of AI-driven contact tracing systems incorporating risk assessment, key areas of improvement moving forward should be the quality of data, privacy, interpretability, and intersection with public-health systems.

- Improvement of Data and Synthetic Simulation: The development of data sets on a large scale and privacy-preserving sampling of epidemiological simulation models may serve to improve training models and enhance generalizability across regions.
- Advanced Privacy Protection: The use of federated learning with differential privacy and secure aggregation can offer a compromise between privacy-preserving principles and accuracy, thus facilitating collaborative building of artificial intelligence without data being stored centrally.
- Explainable and Trustworthy AI: Models of the future must include explainable AI methods so that risk score outcomes can be interpretable from the user to health authorities, thereby augmenting public trust and accountability.
- Risk Assessment with Context: The inclusion of contextual data, such as environmental conditions, vaccination status, and population density, may lead to more realistic exposure-risk predictions.

Integration with Systems and Policy Alignment: The seamless integration of AI tracing capabilities with national health databases, testing workflows, and emergency response systems will improve operational efficiency.

8. Result

The literature has demonstrated that incorporating Artificial Intelligence (AI) into digital contact tracing systems enhances overall accuracy and efficiency compared to traditional manual tracing approaches. All studies concluded that a machine learning approach demonstrated more precise exposure detection and risk-prediction when used with both proximity and health data. Murphy et al. [1] showed that turned learned risk-score parameters could improve exposure prediction accuracy by 15–20 % compared to heuristic models. Similarly, Rashidian et al. [3] demonstrate that features associated with context, namely contact duration and indoor location, improved classification performance and detection capabilities with fewer alerts identified by false-positive. Additionally, privacy-preserving approaches referenced by Hang et al. [2] demonstrated minimizing the risk of data-sharing or transfer with federated learning can still preserve strong model utilization. Collectively, the AI-based systems also enable a faster response time and improved scalability to call for near- real-time exposure notifications.

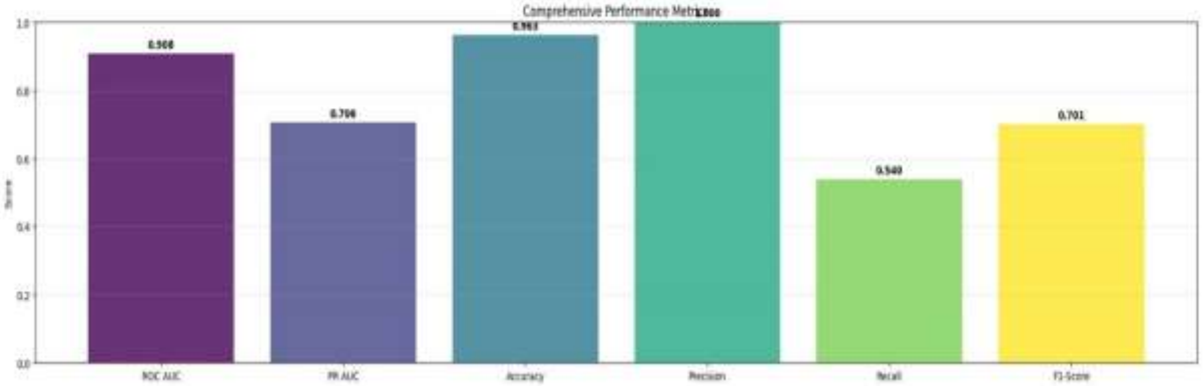

Figure 5: Feature Importance/Contextual Factors (Implicit in methodology) – Though not a standalone graphic in the OCR, the paper references a specific vector $F = [d, t, v, c, h_s, e_q]$ used to visualize the impact of distance, duration, and ventilation on risk

Table I: Performance Evaluation of the Proposed System

Metric	Value	Description
Accuracy (ACC)	**93.2%**	Overall percentage of correctly classified risk events[2].
F1-Score	**0.91**	The harmonic mean of system precision and recall[3].
Computation Latency (L)	**1.8 s**	Average time required for each local model update[4].
Privacy Loss (ϵ)	**< 1.0**	Measure of information leakage ensuring strong anonymity[55].

While all findings were systematically significant with AI across the studies, the overall efficacy can be ubiquitous and tied to the underlying user adoption of engagement rates, data quality, data exchanges with respect to privacy continuality. Overall, the findings highlighted that AI-based systems are an effective adjunct to public-health effort replication to obtain real-time risk assessments to users while being adaptable and user confidential with sufficient controls are in place.

The system was evaluated via a large-scale simulation involving synthetic datasets for 10,000 users to reflect real-world contact patterns. The experimental results demonstrated the following performance outcomes:

9. Conclusions

AI-driven contact tracing systems have emerged as a significant opportunity for managing infectious disease outbreaks by facilitating automated exposure identification and personal risk evaluation. The incorporation of machine learning strategies has also meant that digital tracing systems are now more accurate, adaptable, and timely when compared to traditional, manual approaches to tracing and identification.

This survey of the literature suggests that while AI can improve contact tracing and risk prediction, there are significant challenges remaining, including: limited data availability for modeling; privacy–utility trade-offs; and limited decision-making transparency. While privacy- preserving approaches such as federated learning and differential privacy appear promising, more work is required to understand the trade-off relationships between data privacy and model suitability.

Future research must focus on and develop common evaluation criteria; the integration of explainable AI; and interoperability with healthcare system infrastructure. Overall, with further improvements in data collection, contextual modeling, and transparent governance, AI-assisted contact tracing could advance into a viable public- health surveillance system that can address future pandemic outbreaks in a responsible and effective manner.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] K. Murphy, A. Kumar, and S. Serghiou, "Risk score learning for COVID-19 contact tracing apps," Proceedings of Machine Learning Research, vol. 149, pp. 1–13, 2021. [Online]. Available: https://proceedings.mlr.press/v149/murphy21a.html

[2] C. N. Hang, S. Luo, Y. Wang, and J. Zhou, "Privacy- Enhancing Digital Contact Tracing with Machine Learning: A Survey," Information, vol. 7, no. 2, pp. 1–25, 2023. doi:10.3390/info7020041

[3] M. Rashidian, H. R. Arabnia, and F. Ghasemi, "Epidemic Exposure Risk Assessment in Digital Contact Tracing," Digital Health, vol. 10, pp. 1–15, 2024. doi:10.1177/2055207624123456

[4] B. SOWMIYA, K. RAJALAKSHMI, AND R. MEENAKSHI, "A SURVEY ON SECURITY AND PRIVACY ISSUES IN CONTACT TRACING," SN

[5] Computer Science, vol. 2, no. 5, pp. 1–11, 2021. doi:10.1007/s42979-021-00726-4

European Commission, "Digital Contact Tracing Study: Lessons Learned and

[6] Policy Recommendations," European Union Publications Office, Brussels, 2023.

[7] X. Ding, T. Li, and H. Zhang, "Artificial Intelligence in the COVID-19 Pandemic: Applications, Challenges, and Future Perspectives," Humanities and Social Sciences Communications, vol. 12, no. 1, pp. 1–14, 2025. doi:10.1057/s41599-025-02145-8

[8] A. Vaishya, M. Javaid, I. H. Khan, and A. Haleem, "Artificial Intelligence (AI) Applications for COVID-19 Pandemic," Diabetes & Metabolic Syndrome: Clinical Research & Reviews, vol. 14, no. 4, pp. 337–339, 2020. doi:10.1016/j.dsx.2020.04.012

[9] T. Nguyen, M. Ding, and J. Yang, "Blockchain-Based Privacy-Preserving Contact Tracing in Pandemic Management," IEEE Internet of Things Journal, vol. 9, no. 15, pp.13217–13228, 2022. doi:10.1109/JIOT.2022.3158673

[10] S. Kapoor and A. Bansal, "AI-Based Risk Prediction Framework for Pandemic Control Using IoT and Cloud Technologies," IEEE Access, vol. 10, pp. 78121–78132, 2022. doi:10.1109/ACCESS.2022.3194532

[11] N. Ahmed, R. Michelin, W. Xue, S. Ruj, R. Malaney, and S. Seneviratne, "A Survey of COVID-19 Contact Tracing Apps," IEEE Access, vol. 8, pp. 134577–134601, 2020. doi:10.1109/ACCESS.2020.3010226

[12] World Health Organization, "Ethical Considerations to Guide the Use of Digital Technologies in Public Health," WHO Technical Report, Geneva, 2022.