Rishabh Gupta

Department of Computer Applications
National Institute of Technology
Kurukshetra, Haryana, India

Secure Data Sharing Models in Cloud Environments

My Research Journey

- 2015 –Prof. Ashutosh Kumar Singh's Research Lab
  - As a PhD Scholar (4 Years and 5 Months) since 2018

My Research Journey

- 2015 –Prof. Ashutosh Kumar Singh's Research Lab
  - As a PhD Scholar (4 Years and 5 Months) since 2018
- Research Outcome
  - Quality matters: 10 SCI Journals papers (6 IEEE Journals)
    - ✓ Accepted: 9 papers (4 IEEE + 4 SCI + 1 Scopus + 2 Others)
    - ✓ Under Review: 2 IEEE Journals
    - ✓ Conferences: 3

My Research Journey

- 2015 –Prof. Ashutosh Kumar Singh's Research Lab
  - As a PhD Scholar (4 Years and 5 Months) since 2018
- Research Outcome
  - Quality matters: 10 SCI Journals papers (6 IEEE Journals)
    - ✓ Accepted: 9 papers (4 IEEE + 4 SCI + 1 Scopus + 2 Others)
    - ✓ Under Review: 2 IEEE Journals
    - ✓ Conferences: 3
- Ph.D. Completed: March 2023

Outline

Outline

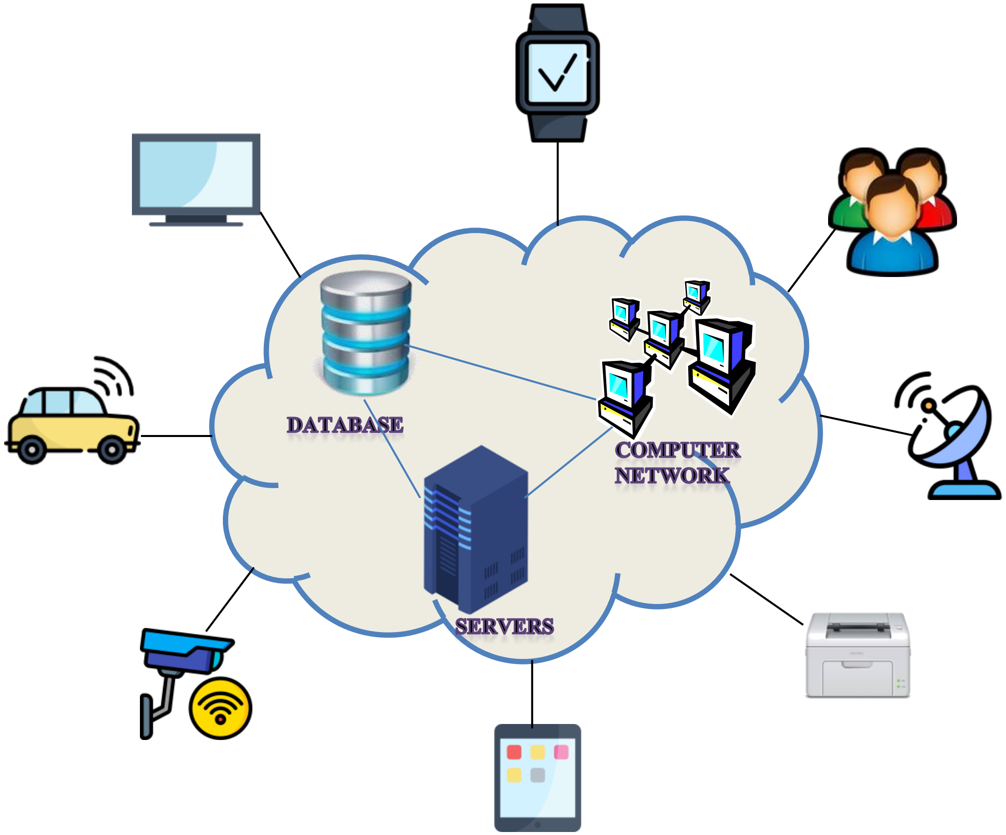
- Introduction and Motivation
  - ✓ Challenges of conventional cloud computing
- Differential Privacy based Data Protection Model
  - ✓ Data Protection and Training
  - ✓ Operational summary
  - ✓ Evaluation and comparison
- Quantum Machine learning based Malicious User Prediction
  - ✓ User Behavior Modeling Unit
  - ✓ Data Preprocessing and Training
  - ✓ QML based Malicious User Analysis Unit
  - ✓ Results and Comparison

Outline

- Introduction and Motivation
  - ✓ Challenges of conventional cloud computing
- Differential Privacy based Data Protection Model
  - ✓ Data Protection and Training
  - ✓ Operational summary
  - ✓ Evaluation and comparison
- Quantum Machine learning based Malicious User Prediction
  - ✓ User Behavior Modeling Unit
  - ✓ Data Preprocessing and Training
  - ✓ QML based Malicious User Analysis Unit
  - ✓ Results and Comparison
- Summary
- Remarks
- References

Cloud Computing

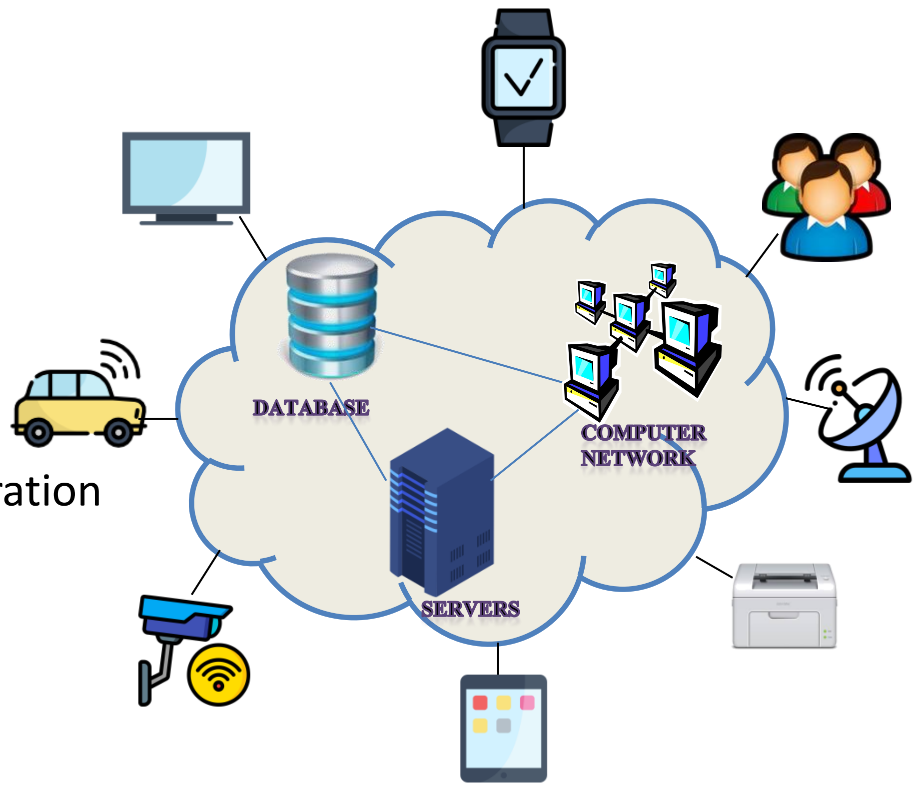
Shared pool of IT resources that are delivered on demand, as service that are: Always on, Accessible from anywhere at anytime.



Cloud Computing

Shared pool of IT resources that are delivered on demand, as service that are: Always on, Accessible from anywhere at anytime.

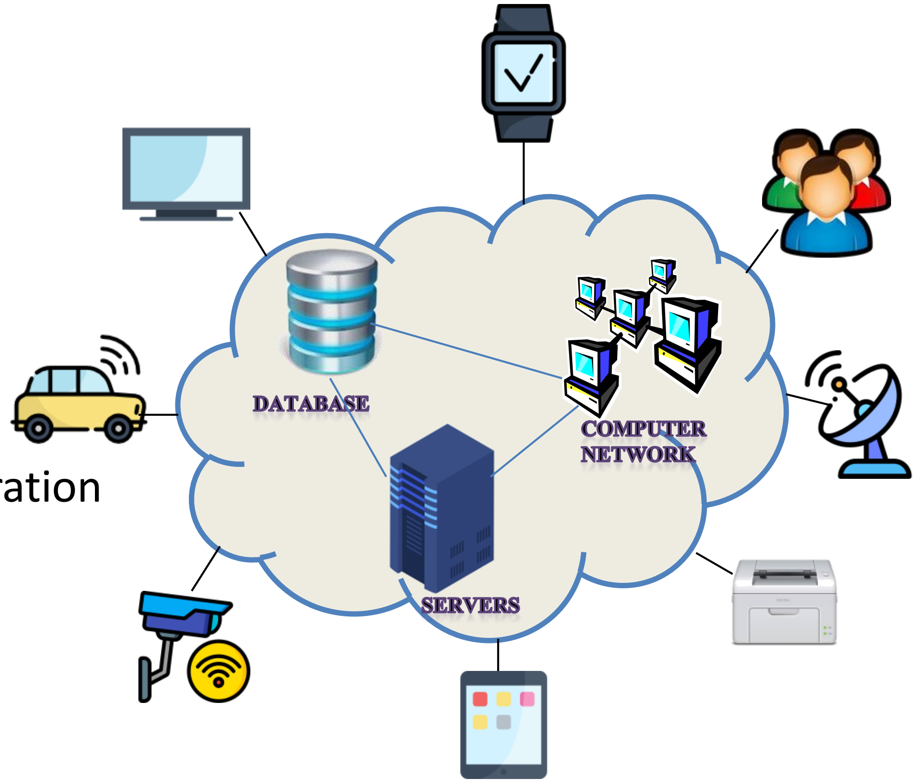
- Cost Saving
- Availability
- Disaster Recovery
- Speed & Scales
- Increased Collaboration



Cloud Computing

Shared pool of IT resources that are delivered on demand, as service that are: Always on, Accessible from anywhere at anytime.

- Cost Saving
- Availability
- Disaster Recovery
- Speed & Scales
- Increased Collaboration

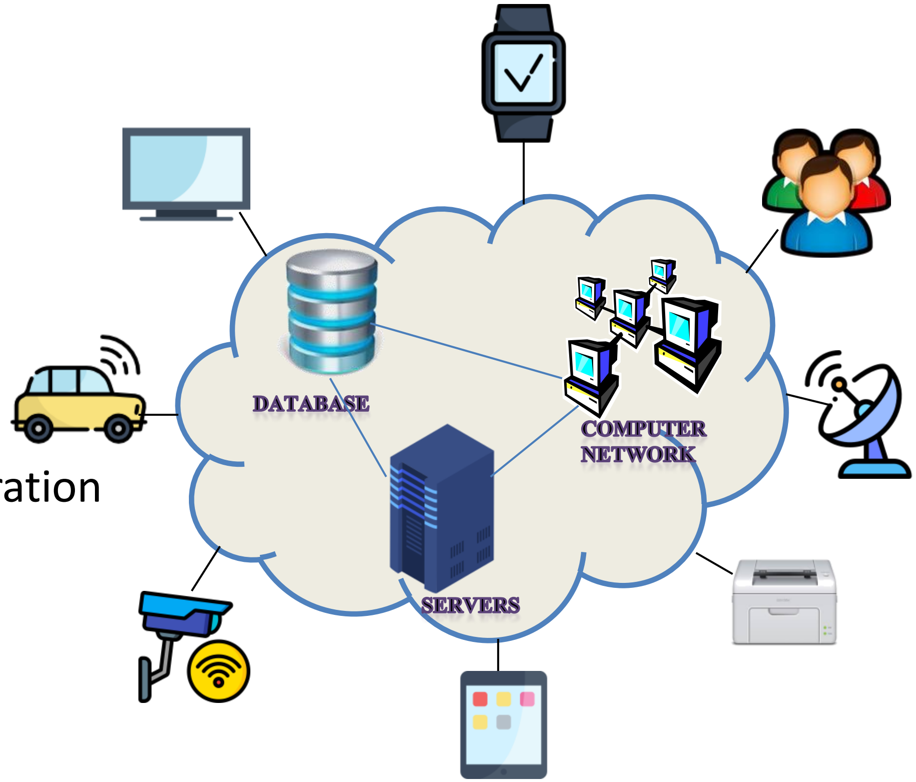


- Data Security
- Data Privacy
- Load Balancing
- Resource Utilization
- Migration
- Power Consumption

Cloud Computing

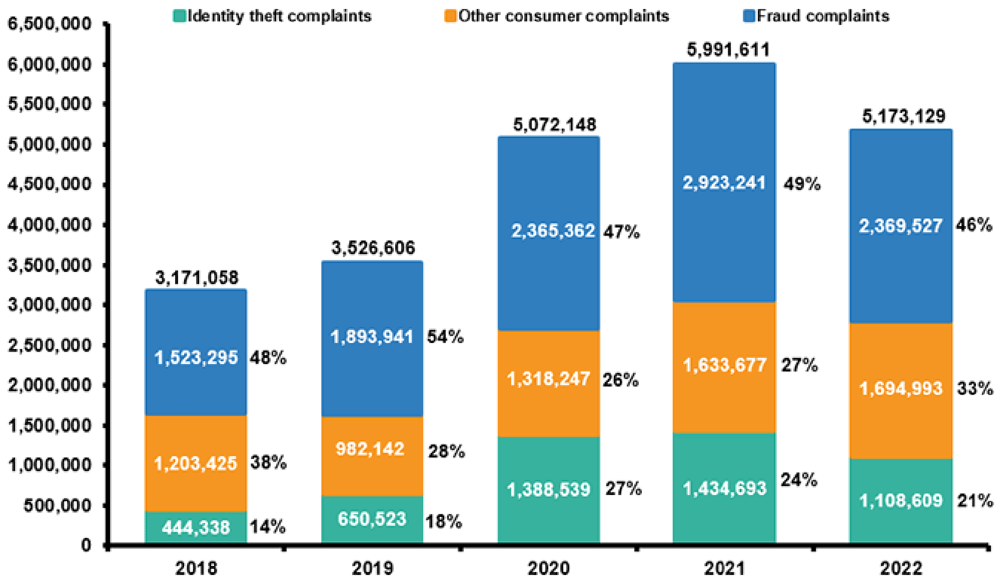
Shared pool of IT resources that are delivered on demand, as service that are: Always on, Accessible from anywhere at anytime.

- Cost Saving
- Availability
- Disaster Recovery
- Speed & Scales
- Increased Collaboration



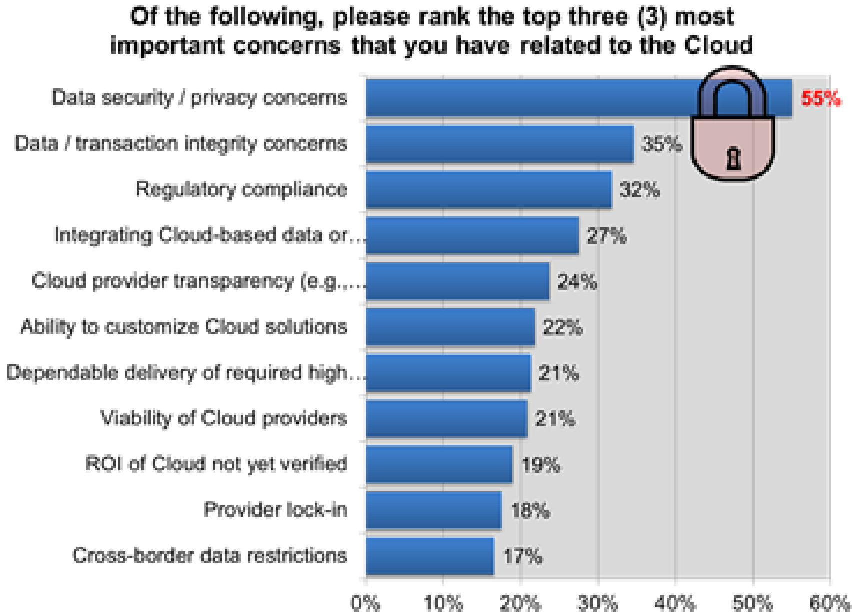
- Data Security
- Data Privacy
- Load Balancing
- Resource Utilization
- Migration
- Power Consumption

Motivation



Identity Theft And Fraud Reports, 2018-2022

https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

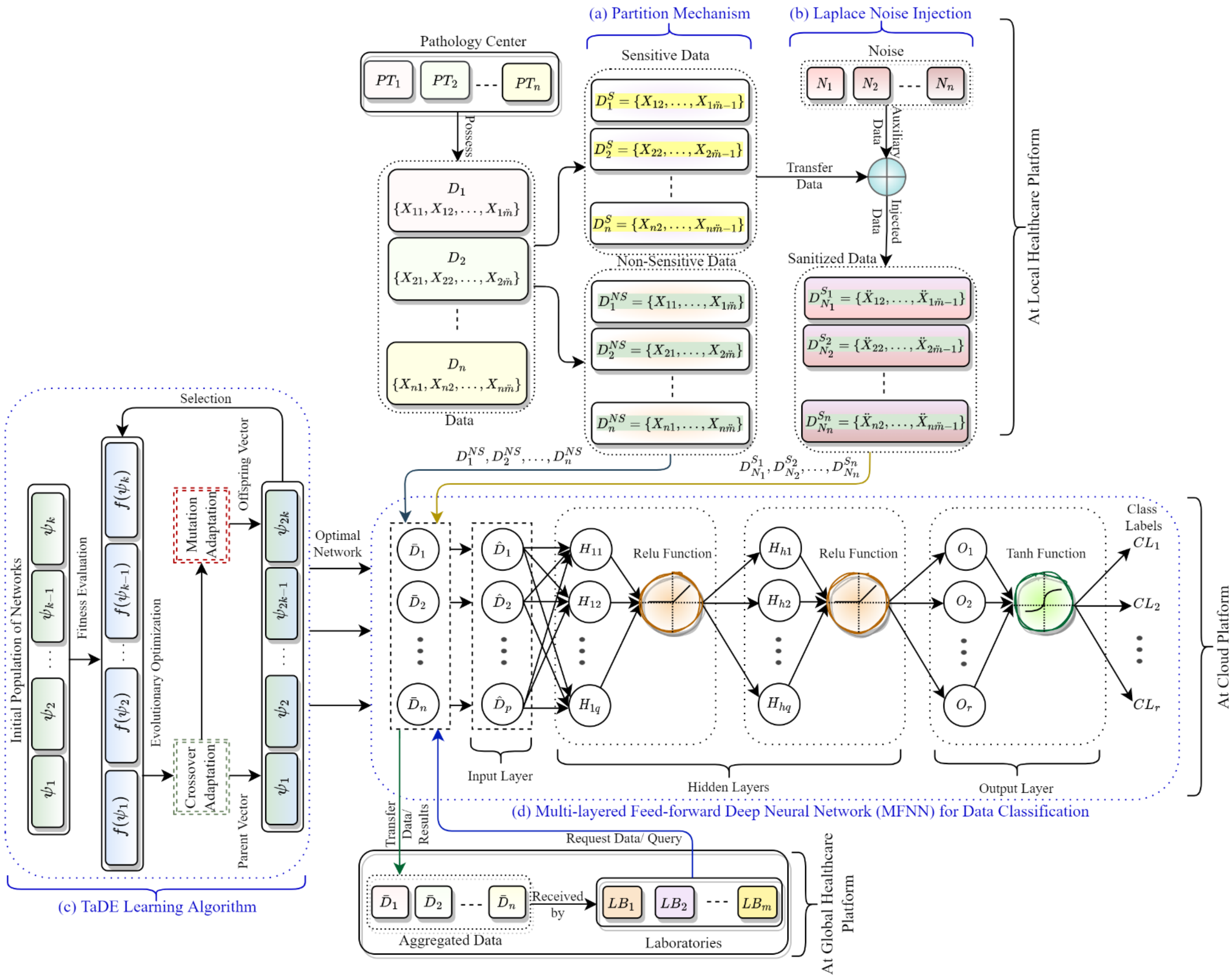


Security as a Top Concern

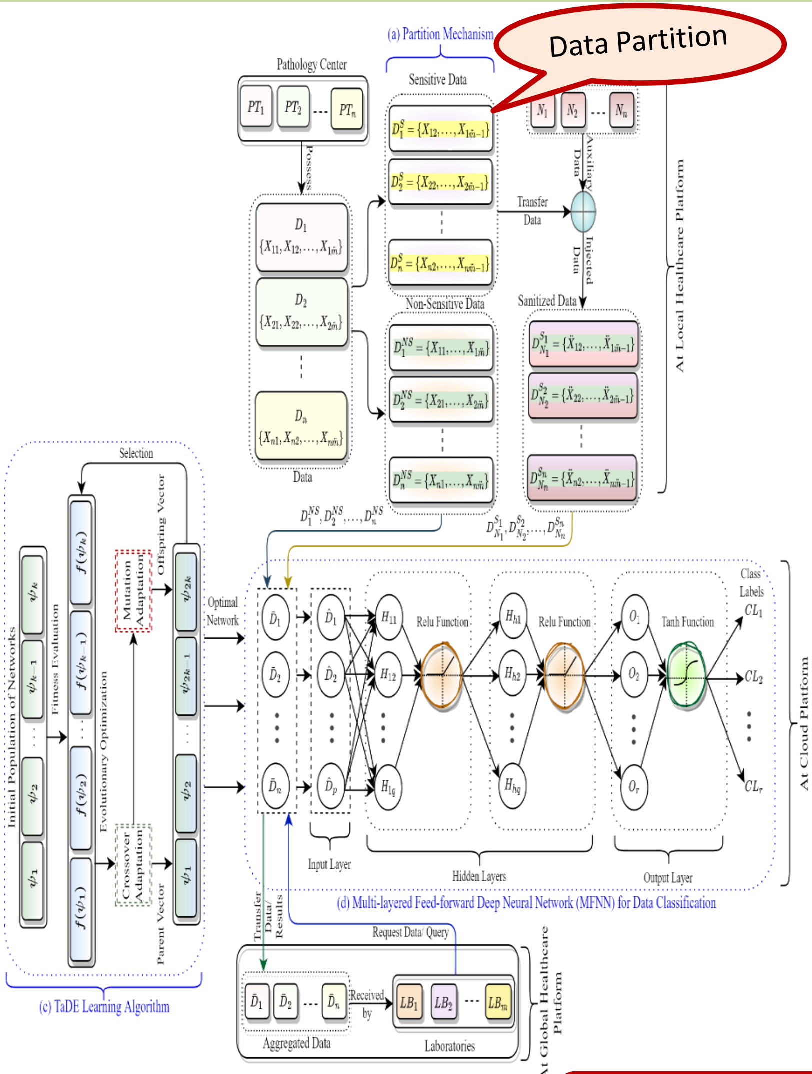
https://www.business2community.com/cloud-computing/why-the-cloud-helps-to-overcome-security-concerns-0591171

Differential Privacy and TriPhase Adaptive Learning based Data Privacy-Preserving Model

Proposed Model



Proposed Model



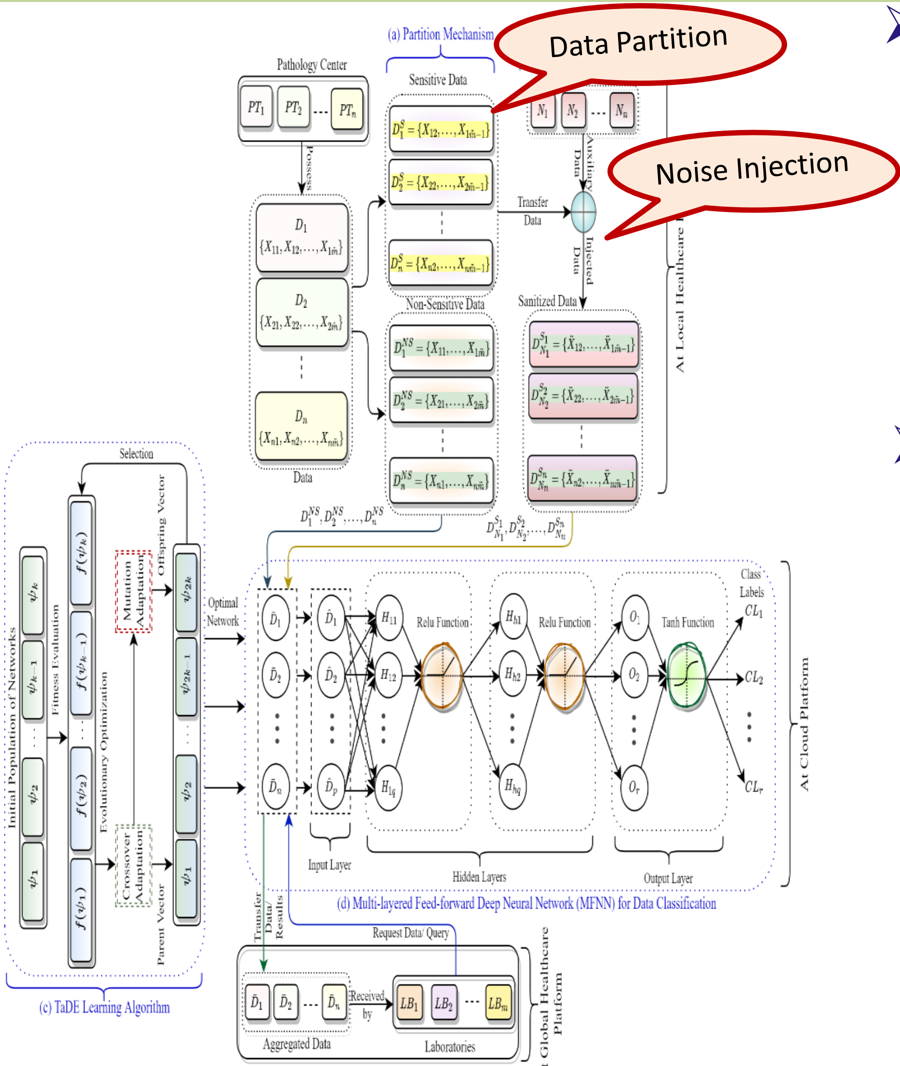
- **Data Partition**
  - ✓ Sensitive and Non-Sensitive

$$SD_1^I = \prod_{(S_1,S_2,\ldots,S_\chi)} (D_1^I)$$

$$ND_1^I = \prod_{(NS_1,NS_2,\ldots,NS_\tau)} (D_1^I)$$

SI : *Sensitive Data*   ND : *Non-Sensitive Data*

Proposed Model



➢ Data Partition

- ✓ Sensitive and Non-Sensitive

$$SD_1^I = \prod_{(S_1,S_2,\ldots,S_\chi)} (D_1^I)$$

$$ND_1^I = \prod_{(NS_1,NS_2,\ldots,NS_\tau)} (D_1^I)$$

➢ Data Protection

- ✓ ε-Differential Privacy

$$Pr\left[\hat{R}(D) = \vartheta\right] \le exp(\epsilon) \times Pr\left[\hat{R}(D') = \vartheta\right]$$

- ✓ Sensitivity

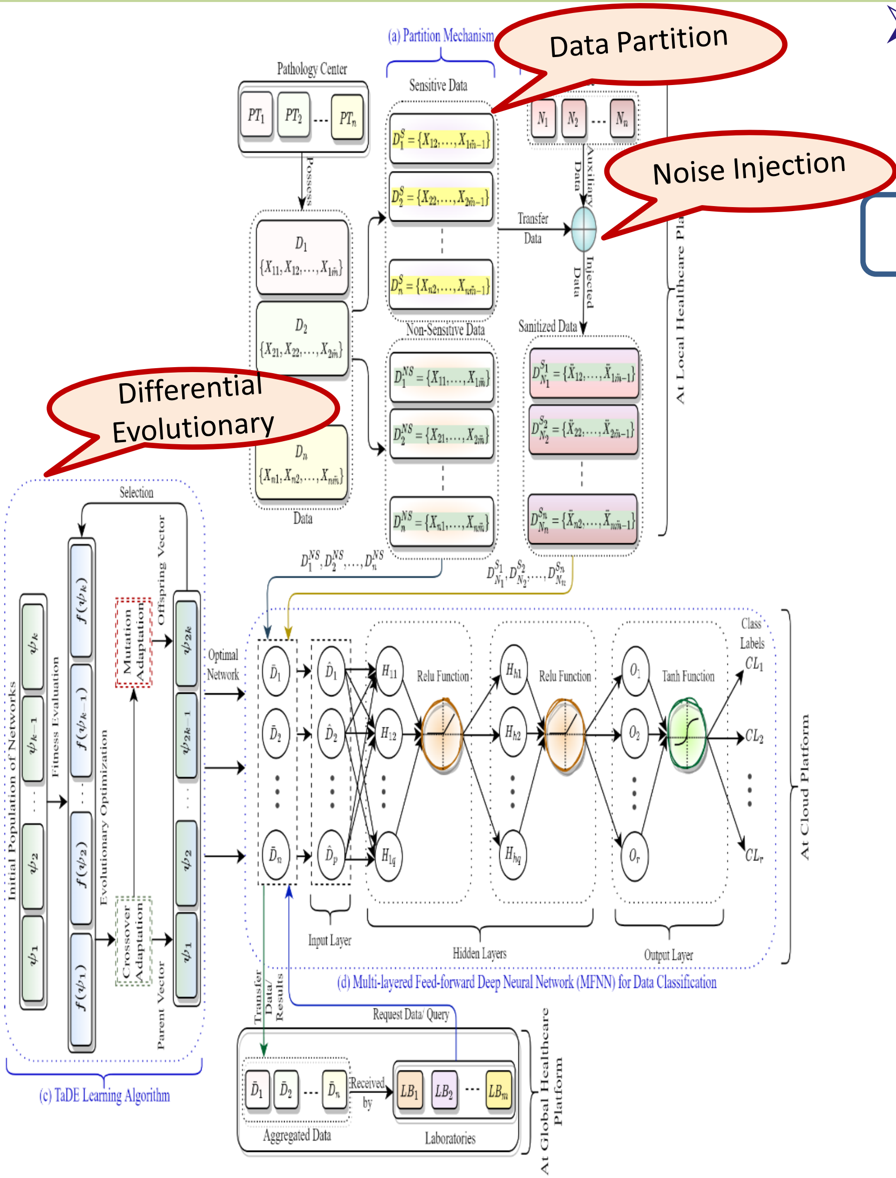
$$\Delta f = \max 1_{D,D'} \parallel f(D) - f(D') \parallel_{P_1}$$

- ✓ Laplace mechanism

$$\mathrm{N} = \frac{1}{2s} \cdot \left(\exp\left(\frac{-|x-\mu|}{s}\right)\right)$$

SI : *Sensitive Data* ND : *Non-Sensitive Data* s : *Scaling Factor* μ : *mean*

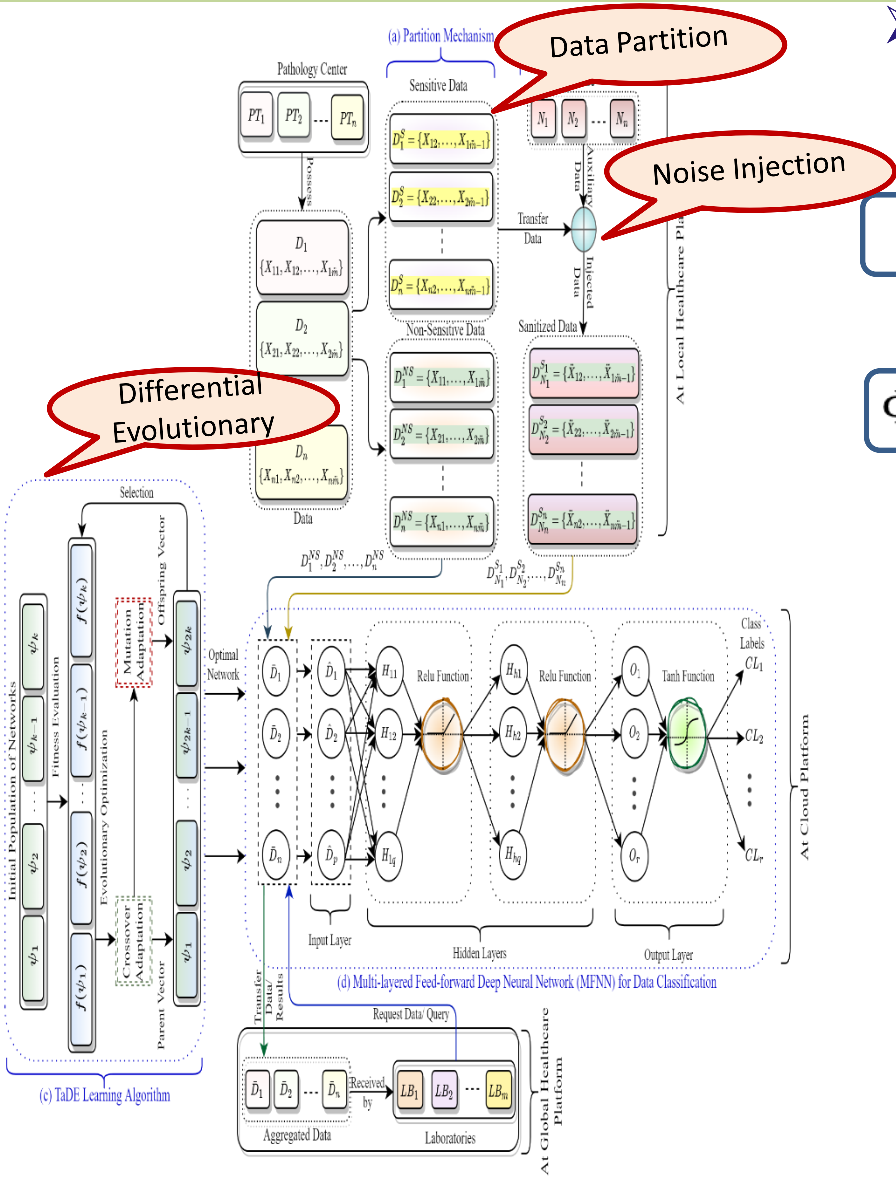
Proposed Model



- **Mutation Strategies**
  - ✓ DE/rand/2

$$\Phi_u^v = \varrho_{r1}^v + \delta_u \times (\varrho_{r2}^v - \varrho_{r3}^v) + \delta_u \times (\varrho_{r4}^v - \varrho_{r5}^v)$$

Proposed Model



Mutation Strategies

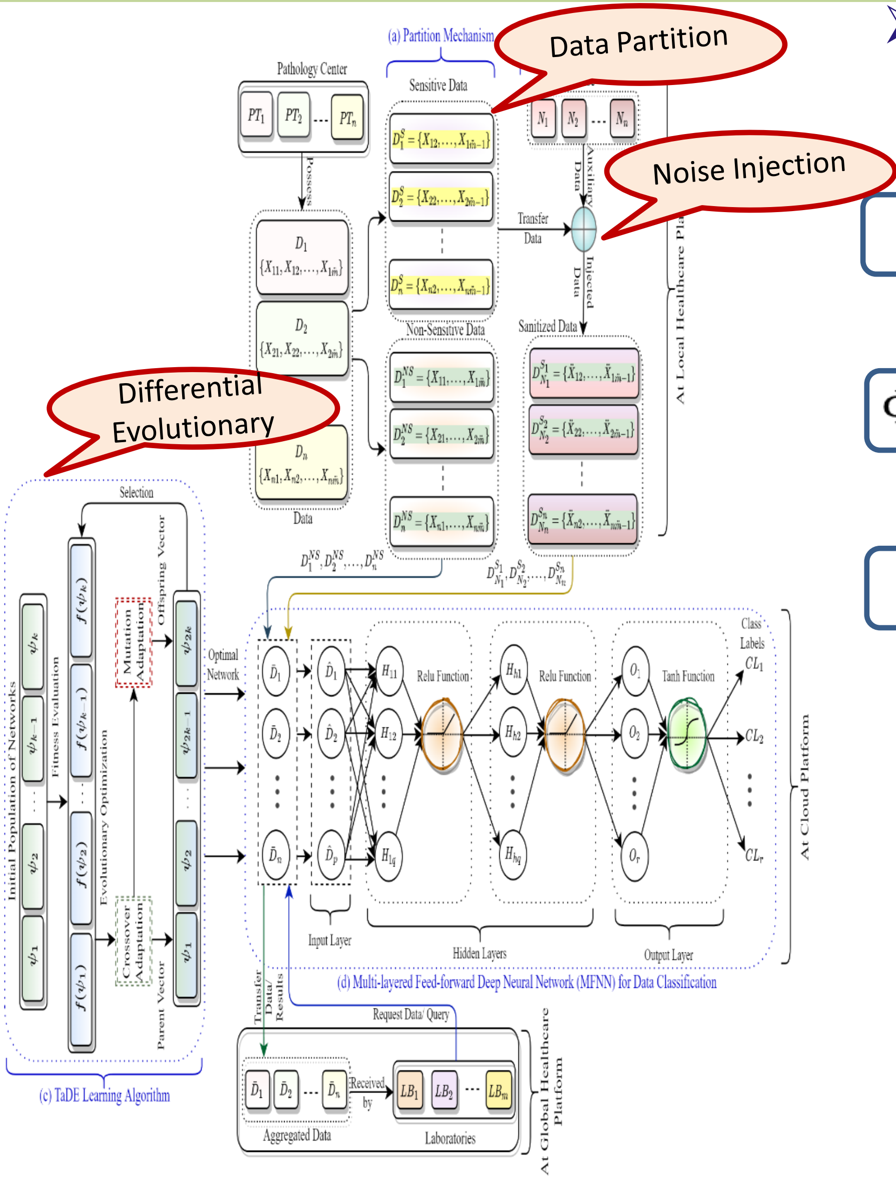
- DE/rand/2

$$\Phi_u^v = \varrho_{r1}^v + \delta_u \times (\varrho_{r2}^v - \varrho_{r3}^v) + \delta_u \times (\varrho_{r4}^v - \varrho_{r5}^v)$$

- DE/best/2

$$\Phi_u^v = \varrho_{best}^v + \delta_u \times (\varrho_{r1}^v - \varrho_{r2}^v) + \delta_u \times (\varrho_{r3}^v - \varrho_{r4}^v)$$

Proposed Model



➢ Mutation Strategies

- ✓ DE/rand/2

$$\Phi_u^v = \varrho_{r1}^v + \delta_u \times (\varrho_{r2}^v - \varrho_{r3}^v) + \delta_u \times (\varrho_{r4}^v - \varrho_{r5}^v)$$

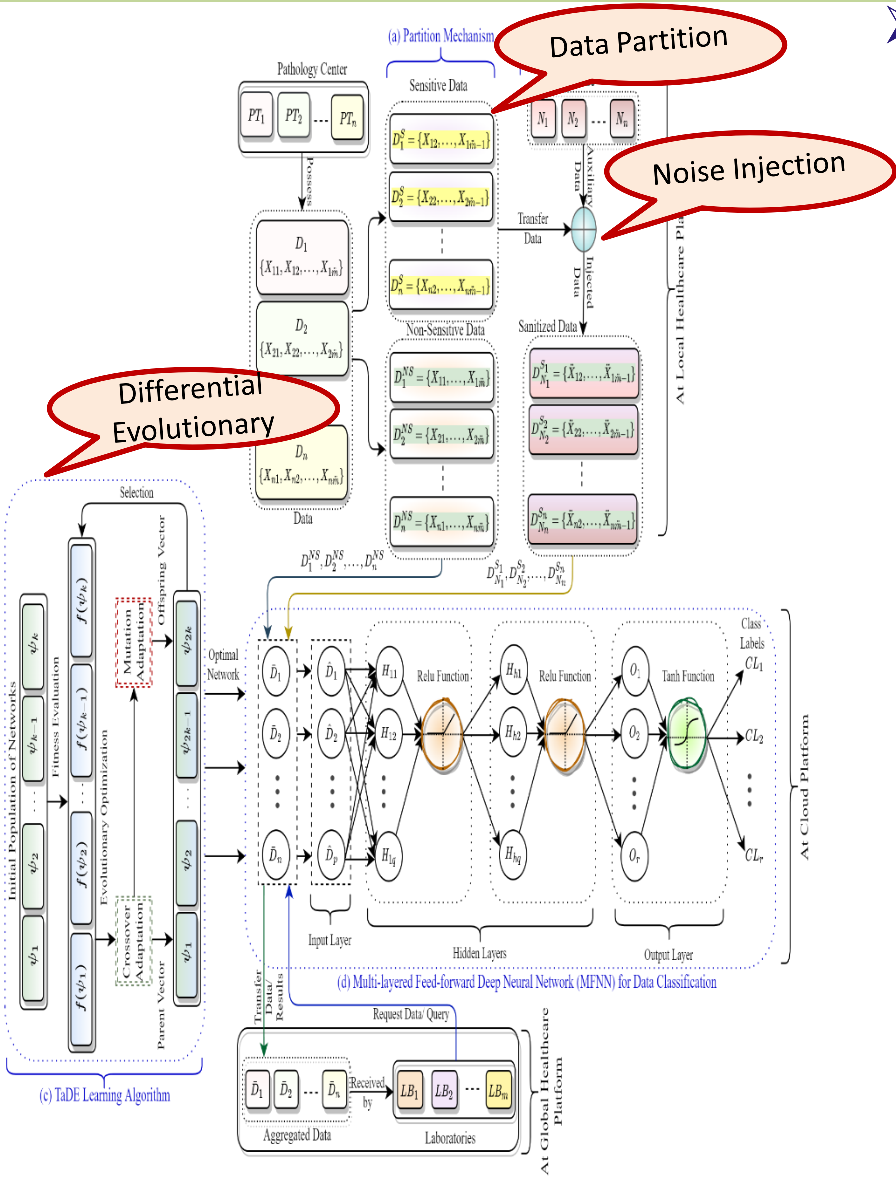
- ✓ DE/best/2

$$\Phi_u^v = \varrho_{best}^v + \delta_u \times (\varrho_{r1}^v - \varrho_{r2}^v) + \delta_u \times (\varrho_{r3}^v - \varrho_{r4}^v)$$

- ✓ DE/current-to-best/2

$$\Phi_u^v = \varrho_u^v + \delta_u \times (\varrho_{best}^v - \varrho_u^v) + \delta_u \times (\varrho_{r1}^v - \varrho_{r2}^v)$$

Proposed Model

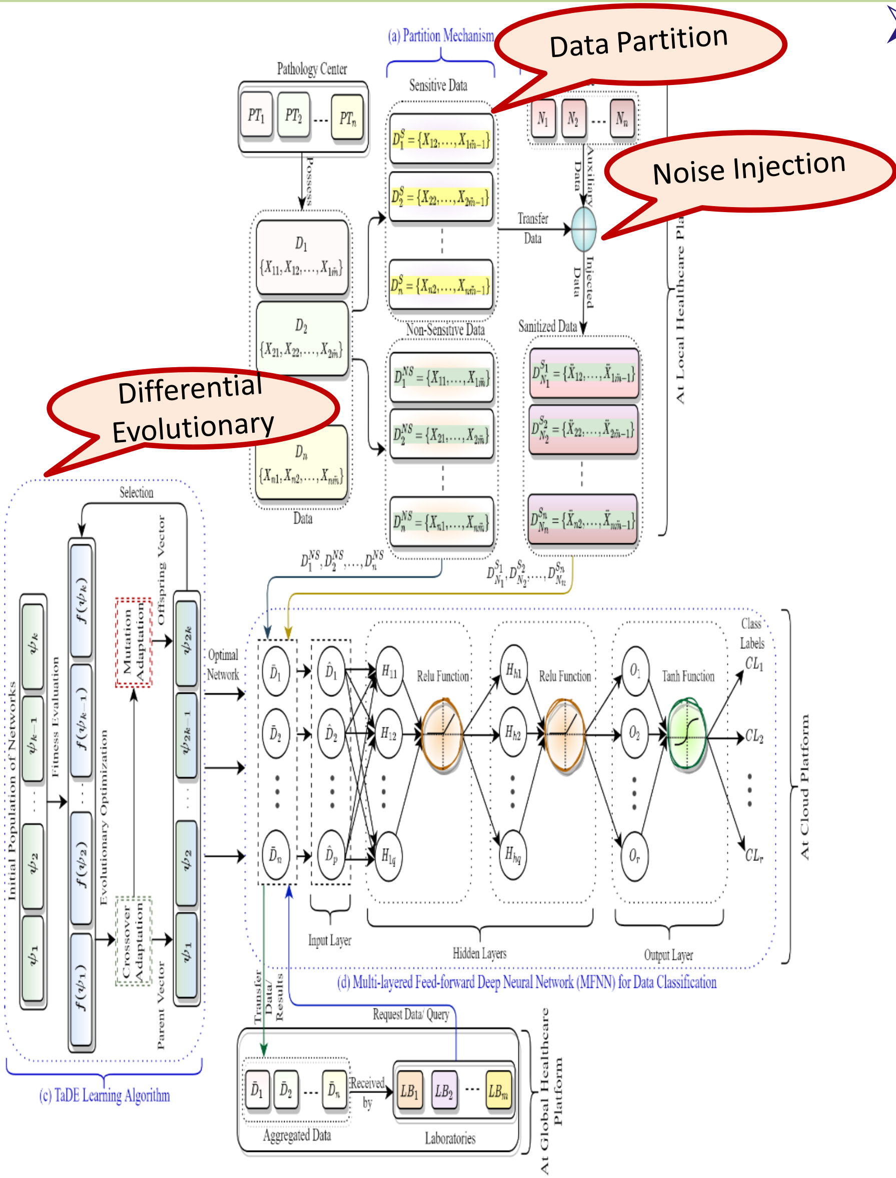


- **Crossover Strategies**
  - ✓ Multi-point

$$\varrho^{u}_{child1} = \begin{cases} \varrho_{2u} & If(k_1 \leq \varrho_{1u} \leq k_2) \\ \varrho_{1u} & otherwise \end{cases}$$

$$\varrho^{u}_{child2} = \begin{cases} \varrho_{1u} & If(k_1 \leq \varrho_{2u} \leq k_2) \\ \varrho_{2u} & otherwise \end{cases}$$

Proposed Model



- ## Crossover Strategies
  - ✓ Multi-point

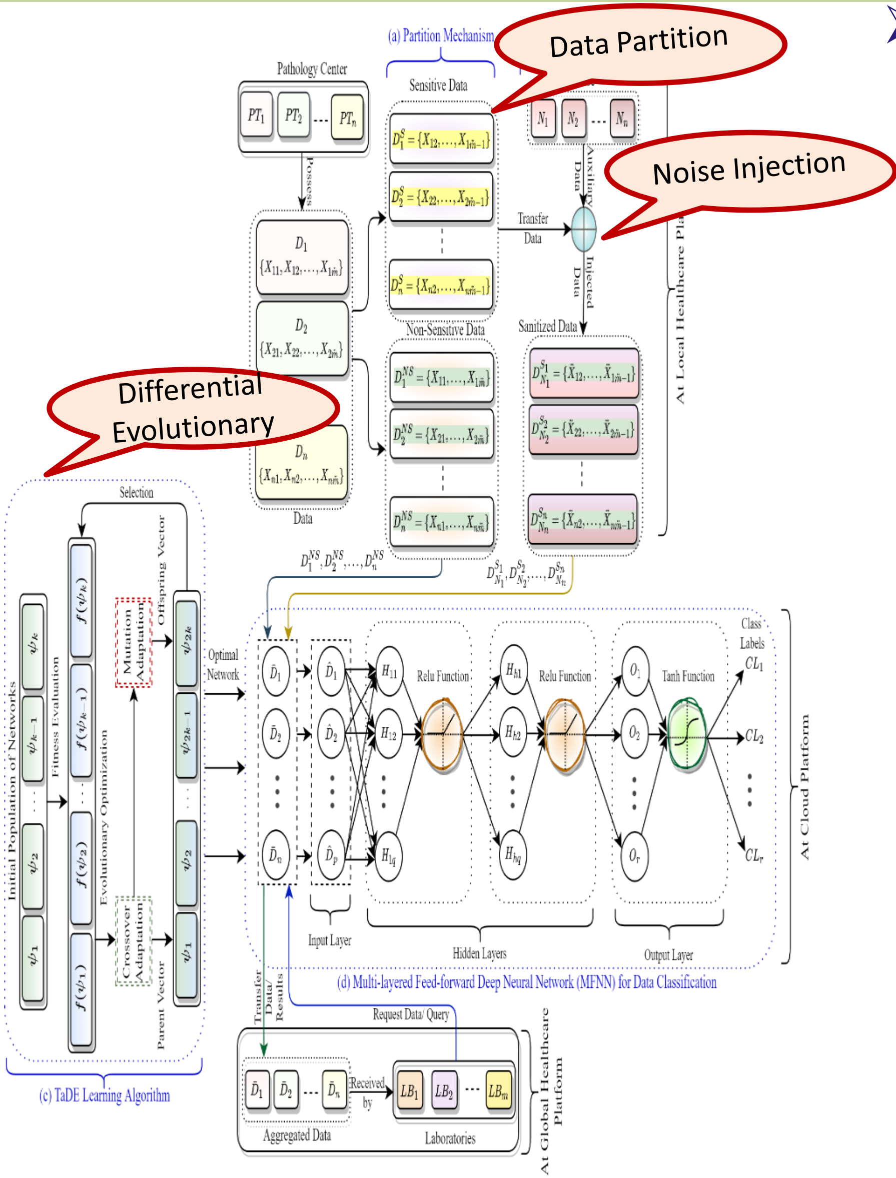
$$\varrho^u_{child1} = \begin{cases} \varrho_{2u} & If(k_1 \le \varrho_{1u} \le k_2) \\ \varrho_{1u} & otherwise \end{cases}$$

$$\varrho^u_{child2} = \begin{cases} \varrho_{1u} & If(k_1 \le \varrho_{2u} \le k_2) \\ \varrho_{2u} & otherwise \end{cases}$$

  - ✓ Ring

$$\varrho^u_{child1} = \mathfrak{B} \times \varrho_{1u} + (L - \mathfrak{B}) \times \varrho_{2u}$$
$$\varrho^u_{child2} = \mathfrak{B} \times \varrho_{2u} + (L - \mathfrak{B}) \times \varrho_{1u}$$

Proposed Model



➢ Crossover Strategies

- ✓ Multi-point

$$\varrho^{u}_{child1} = \begin{cases} \varrho_{2u} & If(k_1 \le \varrho_{1u} \le k_2) \\ \varrho_{1u} & otherwise \end{cases}$$

$$\varrho^{u}_{child2} = \begin{cases} \varrho_{1u} & If(k_1 \le \varrho_{2u} \le k_2) \\ \varrho_{2u} & otherwise \end{cases}$$

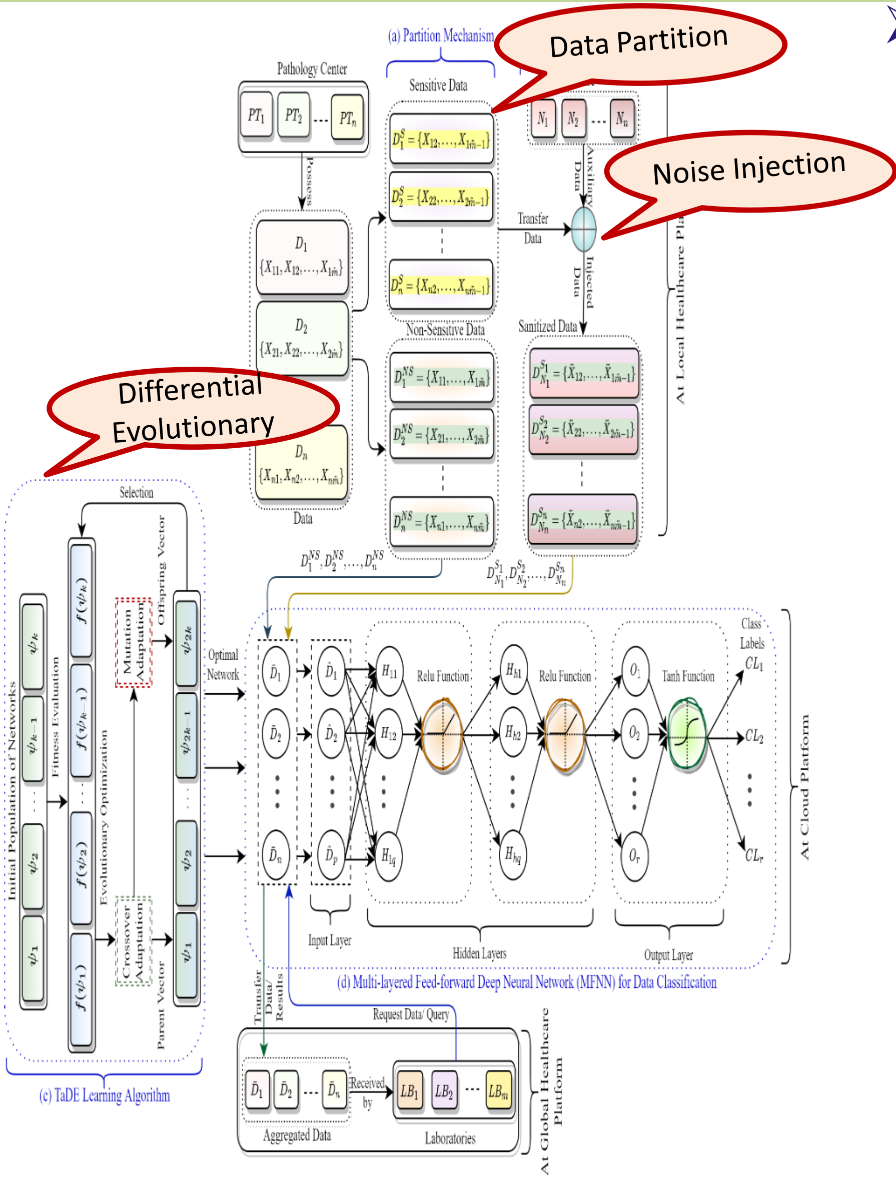
- ✓ Ring

$$\varrho^{u}_{child1} = \mathfrak{B} \times \varrho_{1u} + (L - \mathfrak{B}) \times \varrho_{2u}$$
$$\varrho^{u}_{child2} = \mathfrak{B} \times \varrho_{2u} + (L - \mathfrak{B}) \times \varrho_{1u}$$

- ✓ Heuristic

$$\varrho_{childu} = \delta \times (\varrho_{1u} - \varrho_{2u}) + \varrho_{1u}$$

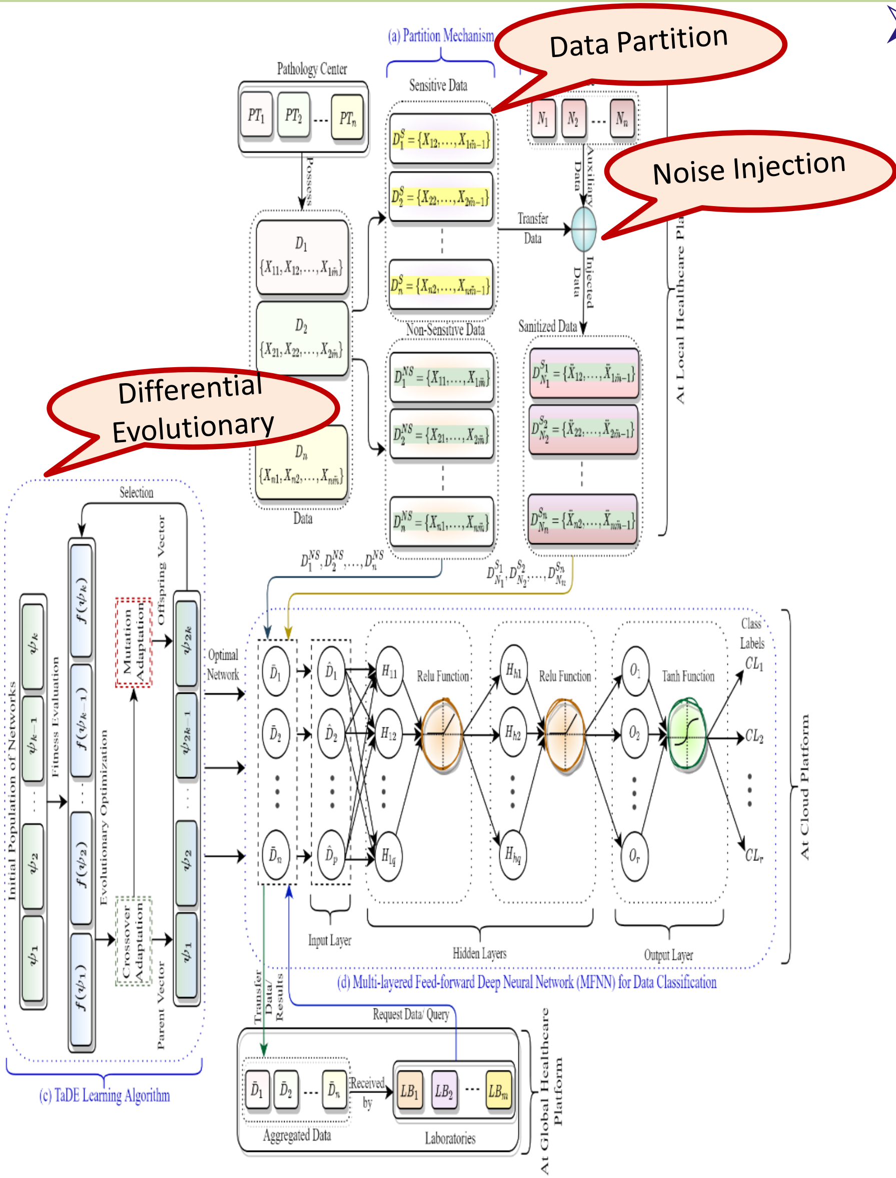
Proposed Model



Control Parameters

$$MR_i^{j+1} = \begin{cases} MR_l + \theta_m (MR_u - MR_l) & (g \leqslant Z) \\ MR_i^j & (otherwise.) \end{cases}$$

Proposed Model



- ## Control Parameters

$$MR_i^{j+1} = \begin{cases} MR_l + \theta_m(MR_u - MR_l) & (g \leqslant Z) \\ MR_i^j & (otherwise.) \end{cases}$$

$$CR_i^{j+1} = \begin{cases} CR_l + \theta_c(CR_u - CR_l) & (g \leqslant Z) \\ CR_i^j & (otherwise.) \end{cases}$$

DT-PPM: Operational Summary

Parameters initialization

Algorithm 1: DT-PPM operational summary

Initialize Pm_1, $Pm_2 = 0.33$, $Pm_3 = 0.34$, Pr_1, $Pr_2 = 0.33$, $Pr_3 = 0.34$
for $i = 1$ *to* n **do**
  $D_i^S = D_i$ - D_i^N, $N_i = \mathrm{Lap}(0,\epsilon)$, $D_{N_i}^{S_i} = D_i^S + N_i$
  Initialize synaptic weight neural network with ψ
  Evaluate each network using fitness function
  for *each solution* v **do**
    Generate mps and cps of ψ
    for *each solution* u **do**
      Generate r_1, r_2, r_3, r_4, and $r_5 \in [1,L]$
      if $0 < mps_u < Pm_1$ **then**
        Apply $DE/rand/2$ mutation
      end
      else if $Pm_1 < mps_u < Pm_1 + Pm_2$ **then**
        Apply $DE/best/2$ mutation
      end
      else
        Apply $DE/current-to-best/2$
      end
      if $0 < cps_u < Pr_1$ **then**
        Apply Multi-point crossover
      end
      else if $Pr_1 < cps_u < Pr_1 + Pr_2$ **then**
        Apply Heuristic crossover
      end
      else
        Apply Ring crossover
      end
    end
    Compute fitness value for each candidates
    Select ω having best fitness value
    Update ms_1, ms_2, ms_3, mf_1, mf_2, and mf_3
    Update Pm_1, Pm_2, Pm_3, Pr_1, Pr_2, and Pr_3
  end
  Apply best population on test data
end
Calculate CA, P, R, and FS

DT-PPM: Operational Summary

Parameters initialization

Noise Injection

Algorithm 1: DT-PPM operational summary

```
Initialize Pm1, Pm2 = 0.33, Pm3 = 0.34, Pr1, Pr2 =
  0.33, Pr3 = 0.34
for i = 1 to n do
    D_i^S = D_i - D_i^N, N_i = Lap(0,ε), D_{N_i}^{S_i} = D_i^S + N_i
    Initialize synaptic weight neural network with ψ
    Evaluate each network using fitness function
    for each solution v do
        Generate mps and cps of ψ
        for each solution u do
            Generate r1, r2, r3, r4, and r5 ∈ [1,L]
            if 0 < mps_u < Pm1 then
                Apply DE/rand/2 mutation
            end
            else if Pm1 < mps_u < Pm1 + Pm2 then
                Apply DE/best/2 mutation
            end
            else
                Apply DE/current − to − best/2
            end
            if 0 < cps_u < Pr1 then
                Apply Multi-point crossover
            end
            else if Pr1 < cps_u < Pr1 + Pr2 then
                Apply Heuristic crossover
            end
            else
                Apply Ring crossover
            end
        end
        Compute fitness value for each candidates
        Select ω having best fitness value
        Update ms1, ms2, ms3, mf1, mf2, and mf3
        Update Pm1, Pm2, Pm3, Pr1, Pr2, and Pr3
    end
    Apply best population on test data
end
Calculate CA, P, R, and FS
```

DT-PPM: Operational Summary

Parameters initialization

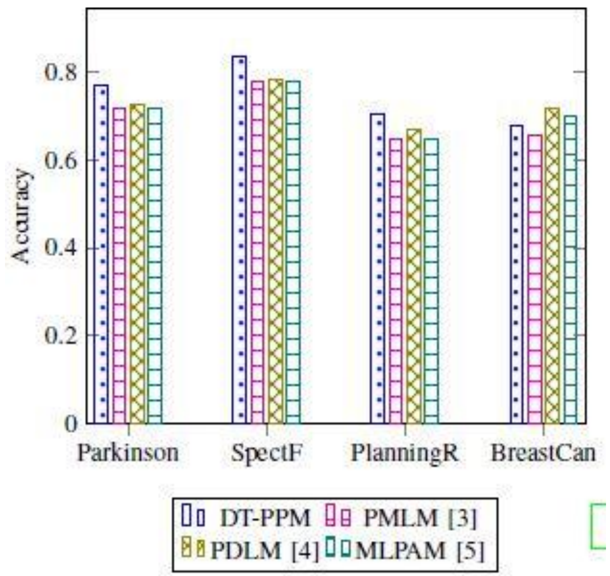
Noise Injection

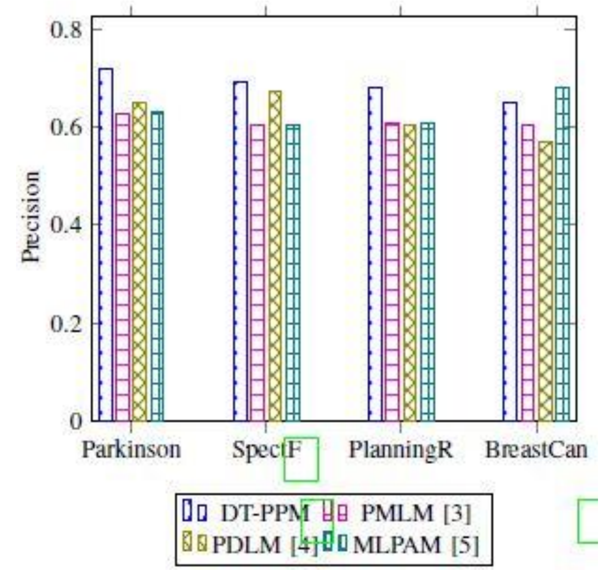
NN Optimization

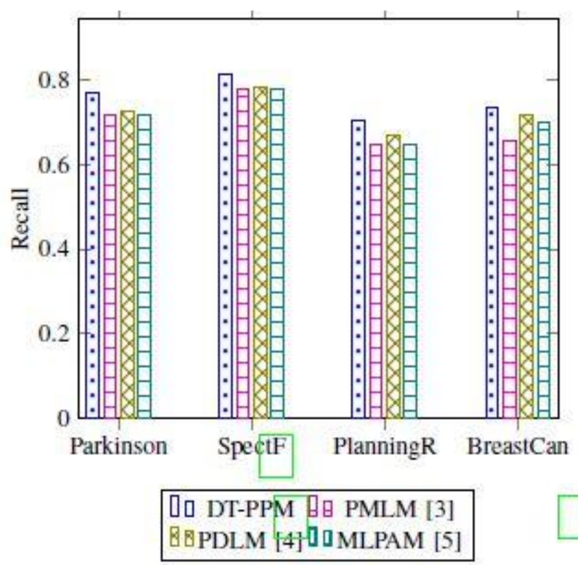
Algorithm 1: DT-PPM operational summary

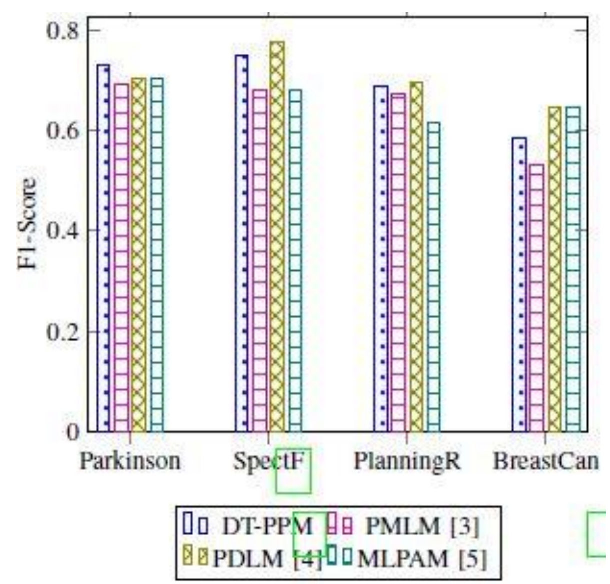
```
Initialize Pm1, Pm2 = 0.33, Pm3 = 0.34, Pr1, Pr2 =
  0.33, Pr3 = 0.34
for i = 1 to n do
    D_i^S = D_i - D_i^N, N_i = Lap(0,ε), D_{N_i}^{S_i} = D_i^S + N_i
    Initialize synaptic weight neural network with ψ
    Evaluate each network using fitness function
    for each solution v do
        Generate mps and cps of ψ
        for each solution u do
            Generate r1, r2, r3, r4, and r5 ∈ [1,L]
            if 0 < mps_u < Pm1 then
                Apply DE/rand/2 mutation
            end
            else if Pm1 < mps_u < Pm1 + Pm2 then
                Apply DE/best/2 mutation
            end
            else
                Apply DE/current − to − best/2
            end
            if 0 < cps_u < Pr1 then
                Apply Multi-point crossover
            end
            else if Pr1 < cps_u < Pr1 + Pr2 then
                Apply Heuristic crossover
            end
            else
                Apply Ring crossover
            end
        end
        Compute fitness value for each candidates
        Select ω having best fitness value
        Update ms1, ms2, ms3, mf1, mf2, and mf3
        Update Pm1, Pm2, Pm3, Pr1, Pr2, and Pr3
    end
    Apply best population on test data
end
Calculate CA, P, R, and FS
```

Classification Results – epsilon-0.1

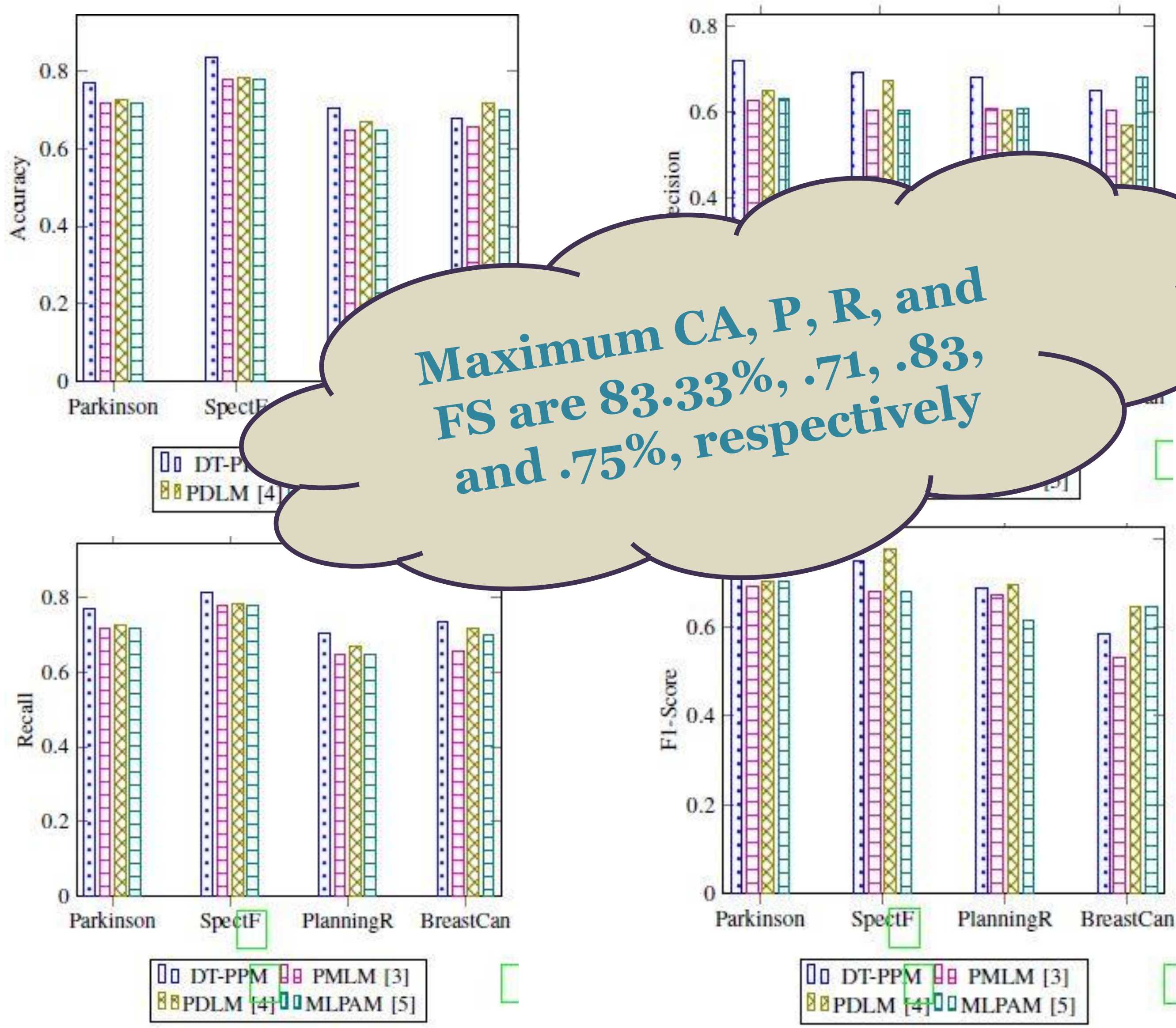






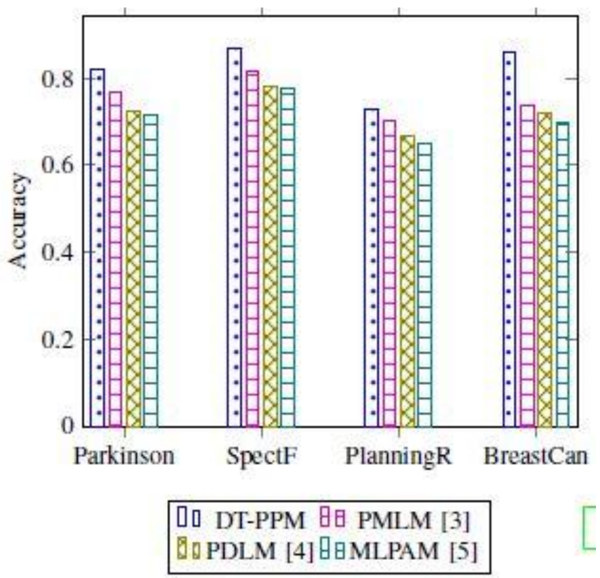


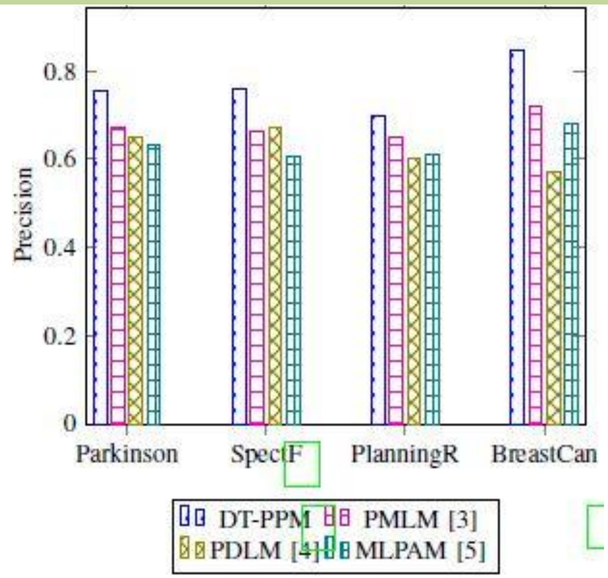
Classification Results – epsilon-0.1

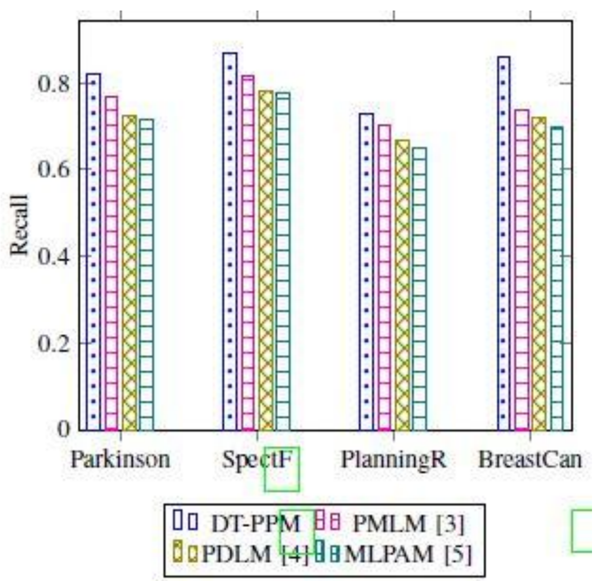


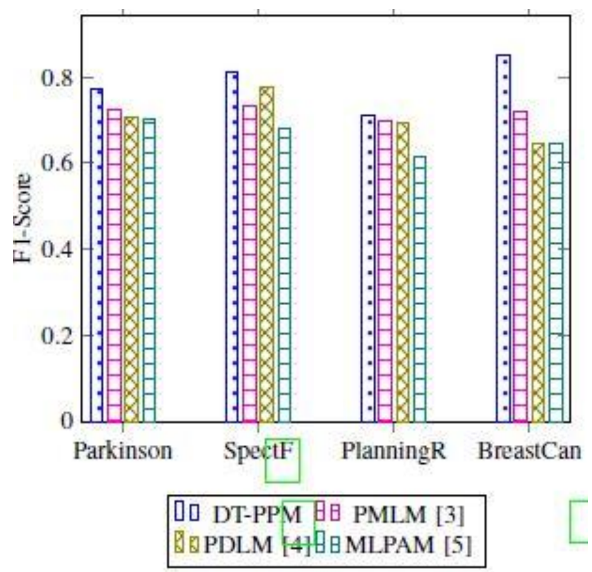
Maximum CA, P, R, and FS are 83.33%, .71, .83, and .75%, respectively

Classification Results – epsilon-1.0

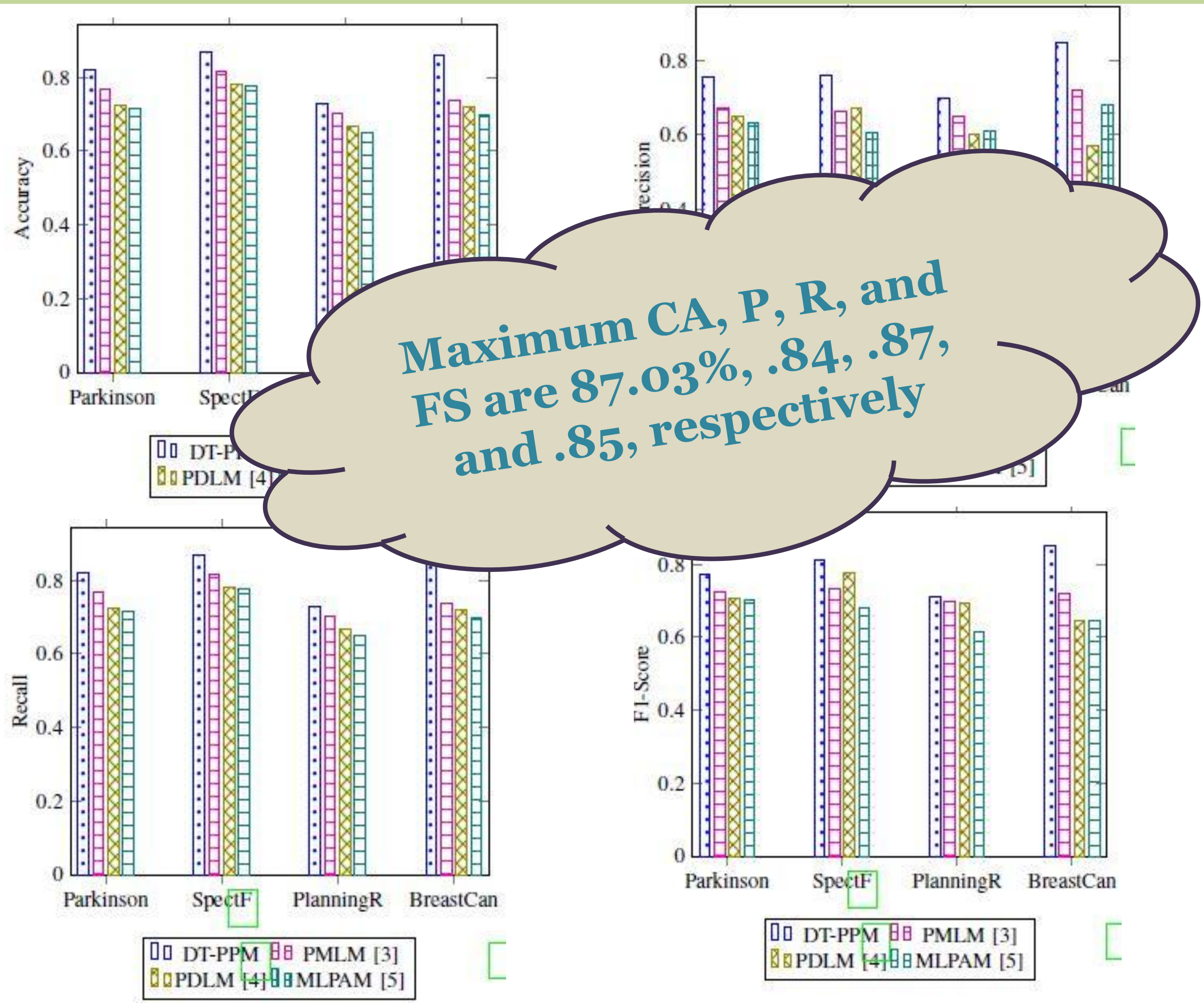








Classification Results – epsilon-1.0



Classification Results

Improvement of privacy parameters of DT-PPM over PMLM, PDLM and MLPAM

Dataset	Accuracy			Precision			Recall			F1-Score		
	[3]	[4]	[5]	[3]	[4]	[5]	[3]	[4]	[5]	[3]	[4]	[5]
Parkinson	5.13	9.61	10.26	8.41	10.55	12.55	5.13	9.61	10.26	5.03	6.68	7.16
SpectF	5.55	8.79	9.26	9.36	8.41	15.26	5.55	8.79	9.26	10.50	3.39	15.61
Planning Relax	2.70	6.04	8.11	4.80	9.33	8.70	2.70	6.04	8.11	6.54	1.63	14.82
Breast Cancer	12.32	13.98	15.89	12.70	27.73	16.57	12.32	13.98	15.89	14.13	20.31	21.44

Classification Results

Improvement of privacy parameters of DT-PPM over PMLM, PDLM, and MLPAM

Dataset	Accuracy			Precision			[illegible]			F1-Score		
	[3]	[4]	[5]	[3]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[3]	[4]	[5]
Parkinson	5.13	9.61	10.26	8.41	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	6.68	7.16
SpectF	5.55	8.79	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	3.39	15.61
Planning Relax	2.70	6.04	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1.63	14.82
Breast Cancer	12.32	13.98	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	14.13	20.31	21.44

Maximum improvements for CA, P, R, and FS are 15.89%, 27.73%, 15.89%, and 21.44%, respectively

Future Scope of Work

Reduction of values of DT-PPM over Clean data

Dataset	Accuracy	Precision	Recall	F1-Score
Parkinson	5.12	0.27	5.12	0.34
SpectF	1.85	3.26	1.85	2.66
Planning Relax	10.81	0.53	10.81	5.24
Breast Cancer	0.57	1.55	0.57	1.02

Future Scope of Work

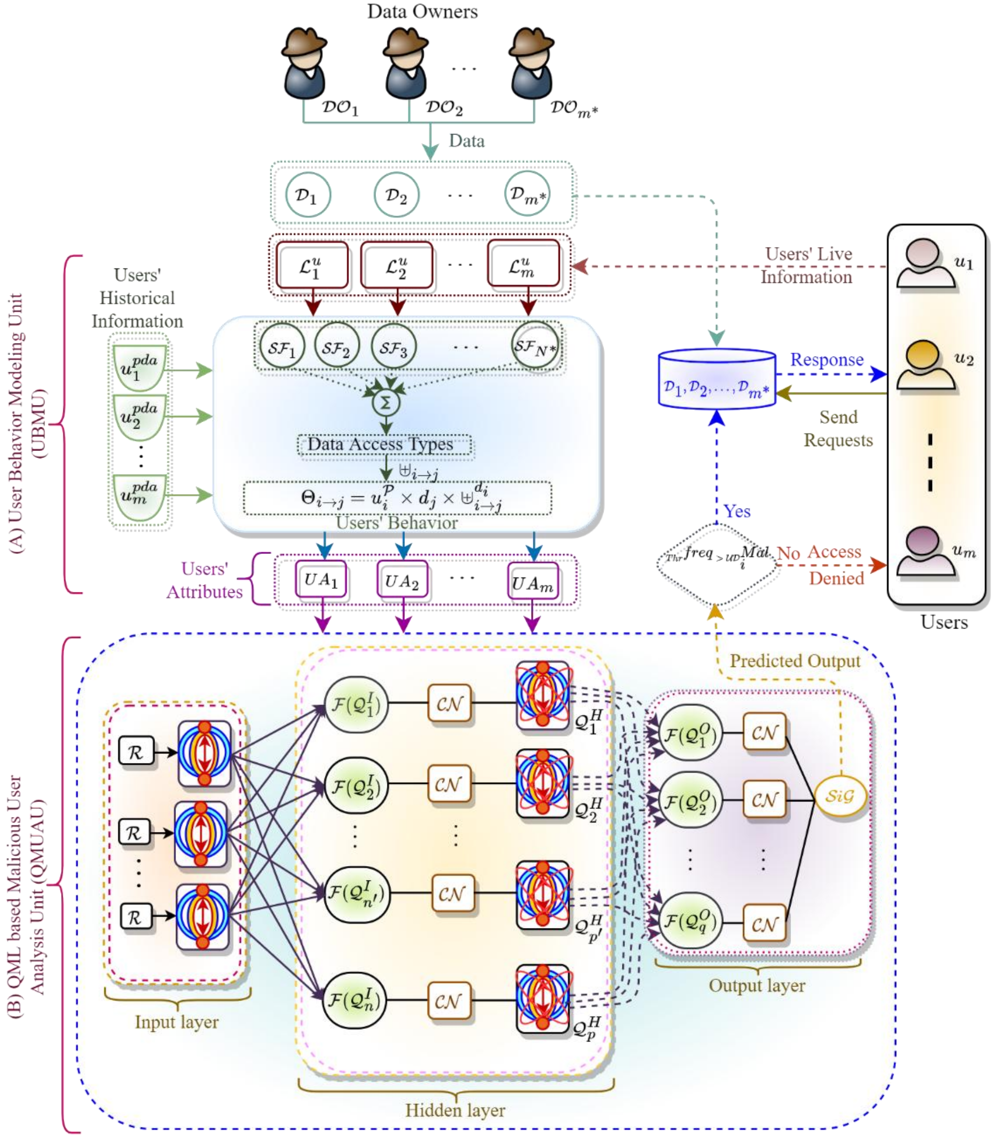
Reduction of values of DT-PPM over Clean data

Dataset	Accuracy
Parkinson	5.12
SpectF	
Plannin	
Breas	

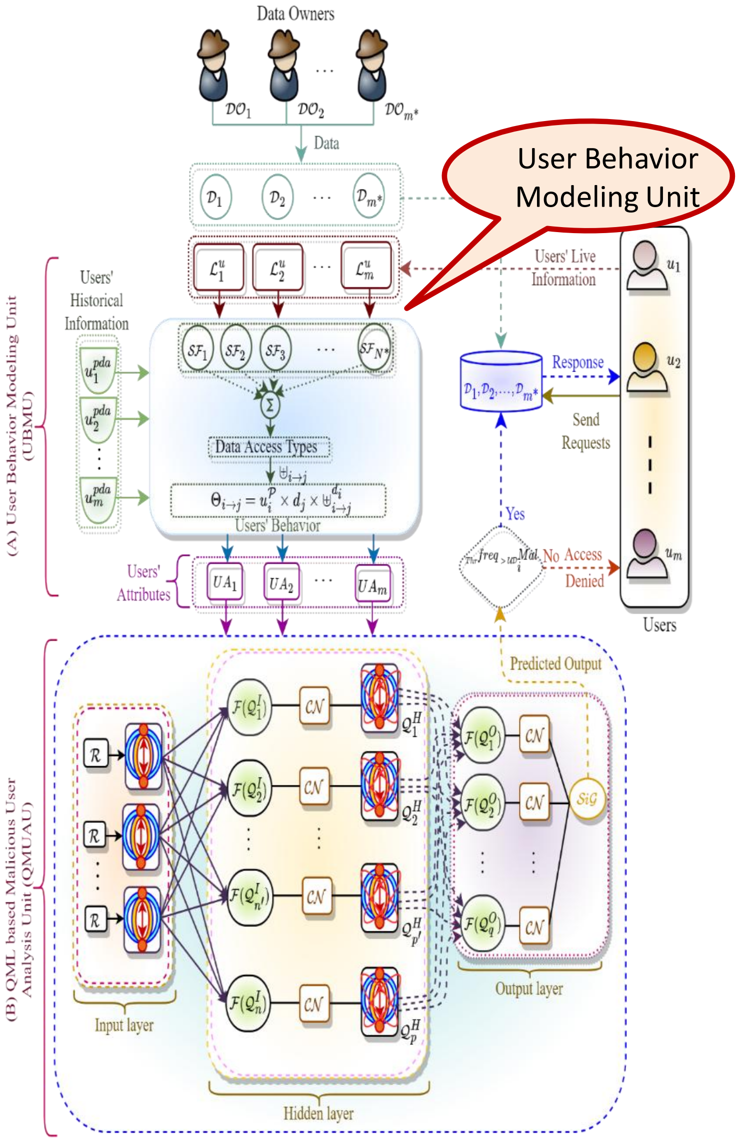
Maximum reductions for CA, P, R, and FS are 10.81%, 3.26%, 10.81%, and 5.24%, respectively

Quantum Machine Learning Driven Malicious User Prediction for Cloud Network Communications

Proposed Model



Proposed Model

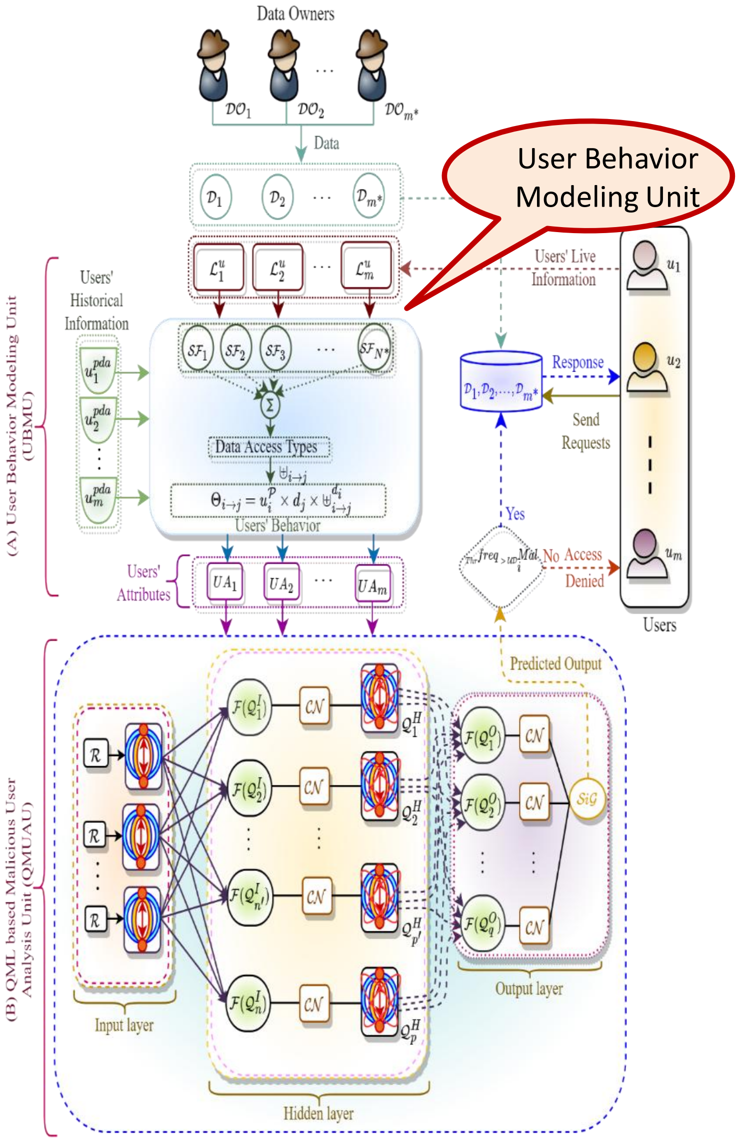


- **User Behavior Modeling Unit**

  - ✓ Historical Data

$$
\mathcal{SF}_{u_i^{pda}} = \begin{cases} Known(0), & \text{If}(|u_i^{pda}| > 0) \\ Unknown(1), & Otherwise \end{cases}
$$

Proposed Model



User Behavior Modeling Unit

- ✓ Historical Data

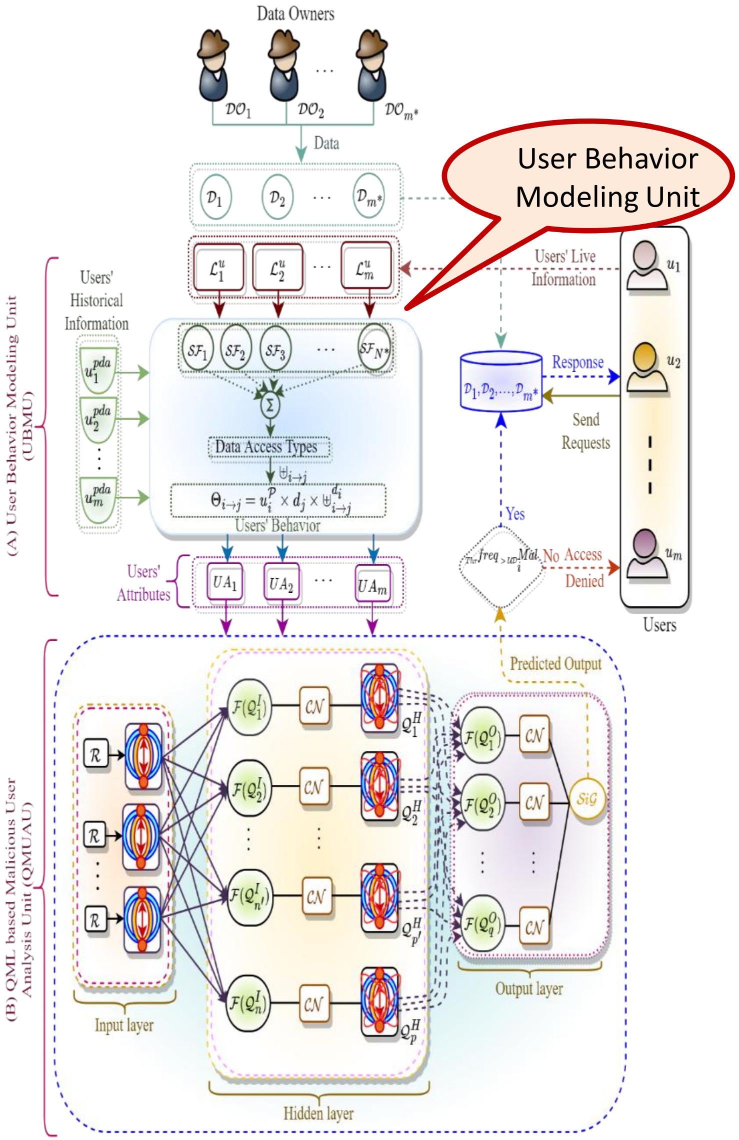
$$\mathcal{SF}_{u_i^{pda}} = \begin{cases} Known(0), & \text{If}(|u_i^{pda}| > 0) \\ Unknown(1), & Otherwise \end{cases}$$

- ✓ Frequently asking data

$$\mathcal{UD}_i^{Mal} = \left| \sum_{k=1}^{H} \sum_{j=1}^{M} dz_k \times t_{ijk} \times u_i \right|$$

$$\mathcal{SF}_{\mathcal{UD}^{Mal}} = \begin{cases} Allowed(0), & If(Thr^{freq} > \mathcal{UD}_i^{Mal}) \\ Denied(1), & Otherwise \end{cases}$$

Proposed Model



➢ User Behavior Modeling Unit

✓ Historical Data

$$\mathcal{SF}_{u_i^{pda}} = \begin{cases} Known(0), & \text{If}(|u_i^{pda}| > 0) \\ Unknown(1), & Otherwise \end{cases}$$

✓ Frequently asking data

$$\mathcal{UD}_i^{Mal} = \left|\sum_{k=1}^{H}\sum_{j=1}^{M} dz_k \times t_{ijk} \times u_i\right|$$

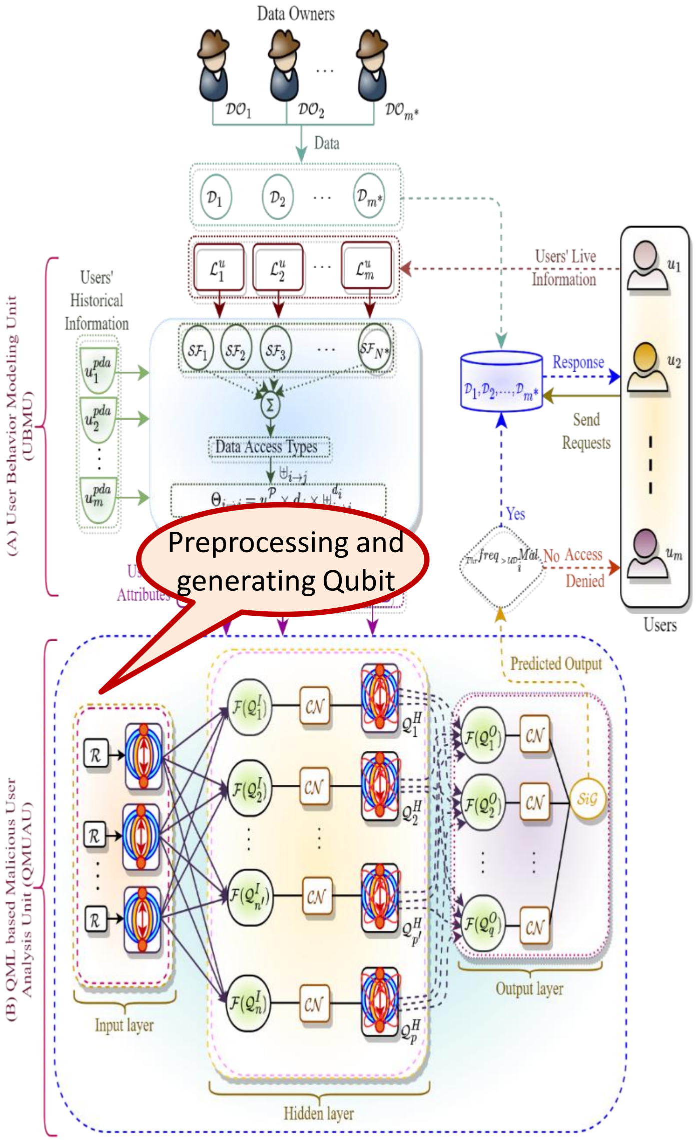
$$\mathcal{SF}_{\mathcal{UD}^{Mal}} = \begin{cases} Allowed(0), & If(Thr^{freq} > \mathcal{UD}_i^{Mal}) \\ Denied(1), & Otherwise \end{cases}$$

✓ Type of Requests

$$\mathcal{AD}_i = (\mathcal{P}_1 \times \sum_{k=1}^{z_1} d_k) \cup (\mathcal{P}_2 \times \sum_{k=1}^{z_2} d_k) \cup \cdots \cup (\mathcal{P}_{m^*} \times \sum_{k=1}^{z_{m^*}} d_k)$$

$$\mathcal{SF}_{\mathcal{AD}_i} = \begin{cases} Authorized(0), & \text{If}(u_i \times (\mathcal{P}_i \times d_i) \subseteq \mathcal{AD}_i) \\ Unauthorized(1), & Otherwise \end{cases}$$

Proposed Model

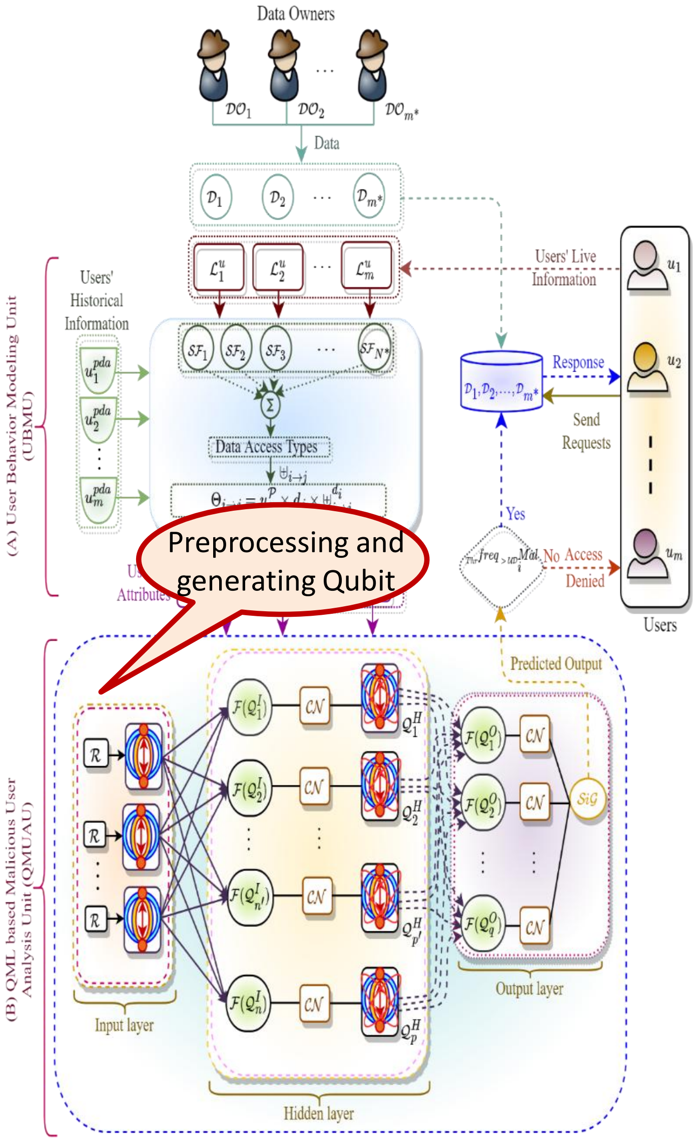


➢ Data Pre-Processing

- ✓ The training input values (UA) are extracted, aggregated, and normalized

$$\hat{UA_j} = \frac{UA_j - UA_{min}}{UA_{max} - UA_{min}}$$

Proposed Model



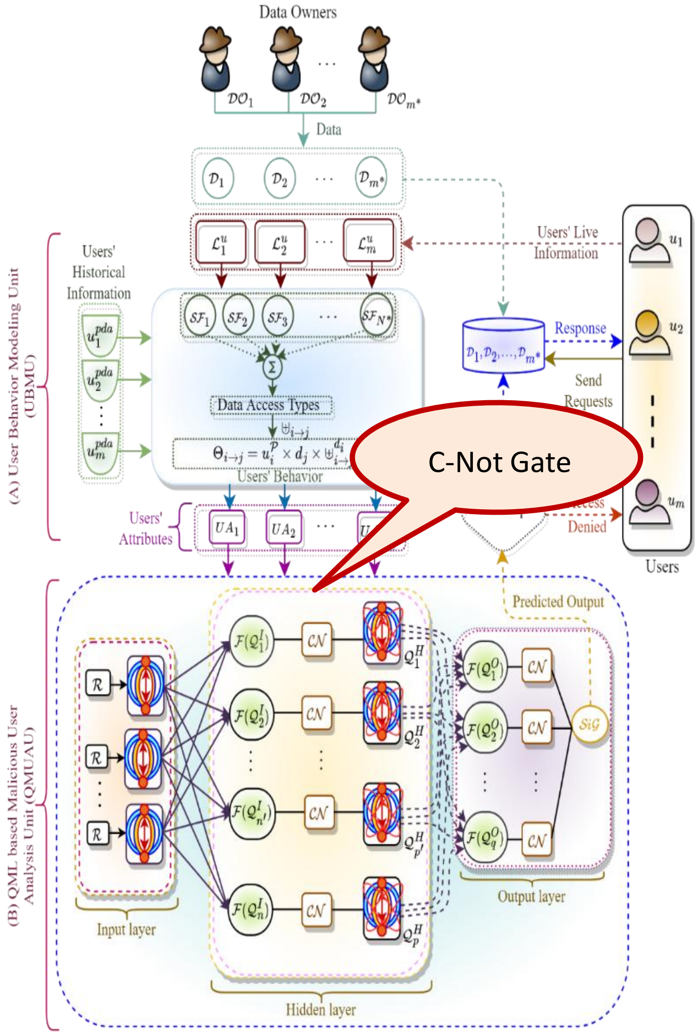
- **Data Pre-Processing**
  - ✓ The training input values (UA) are extracted, aggregated, and normalized

$$\hat{UA}_j = \frac{UA_j - UA_{min}}{UA_{max} - UA_{min}}$$

- **At Input layer, Qubit generation**
  - ✓ Converted into Qubits (Θ) by applying rotation effect

$$\Theta = \frac{\pi}{2} \times \hat{D}$$

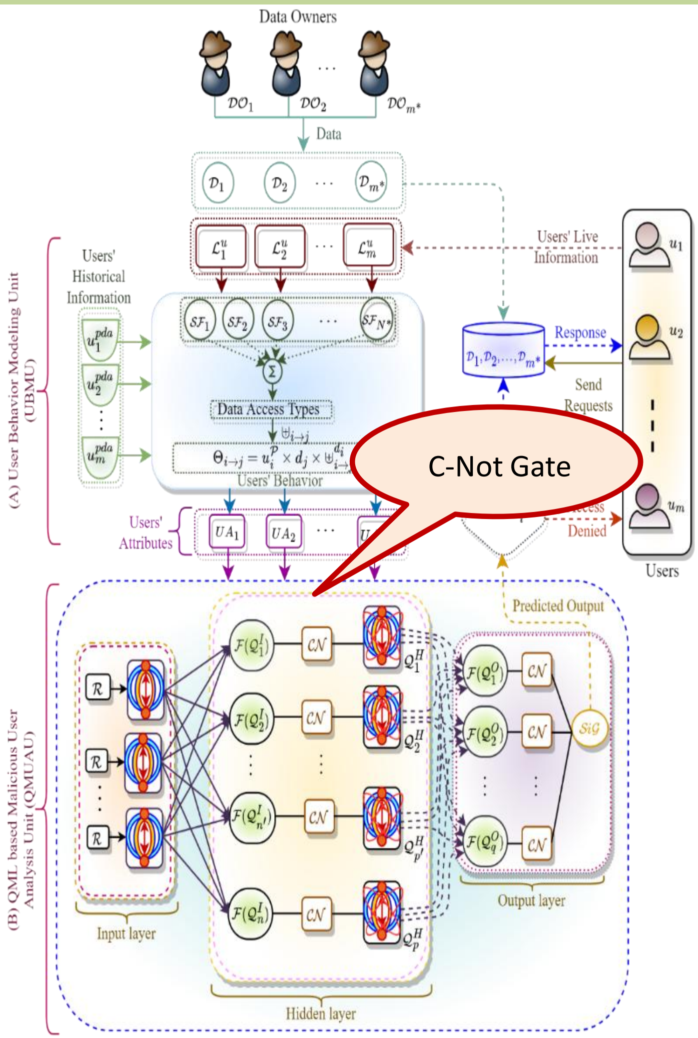
Proposed Model



- **QNN Information Processing**
  - ✓ At Hidden layer, Qubit vector is obtained by applying C-Not gate effect as an activation function

ϖ : *Qubit weight* $\mathcal{B}^I$: *Bias* $\mathcal{G}(\delta^H)$: *Sigmoid function* $arg(Q^{*H}_j)$: *Amplitude of qubit vector*

Proposed Model



➢ QNN Information Processing

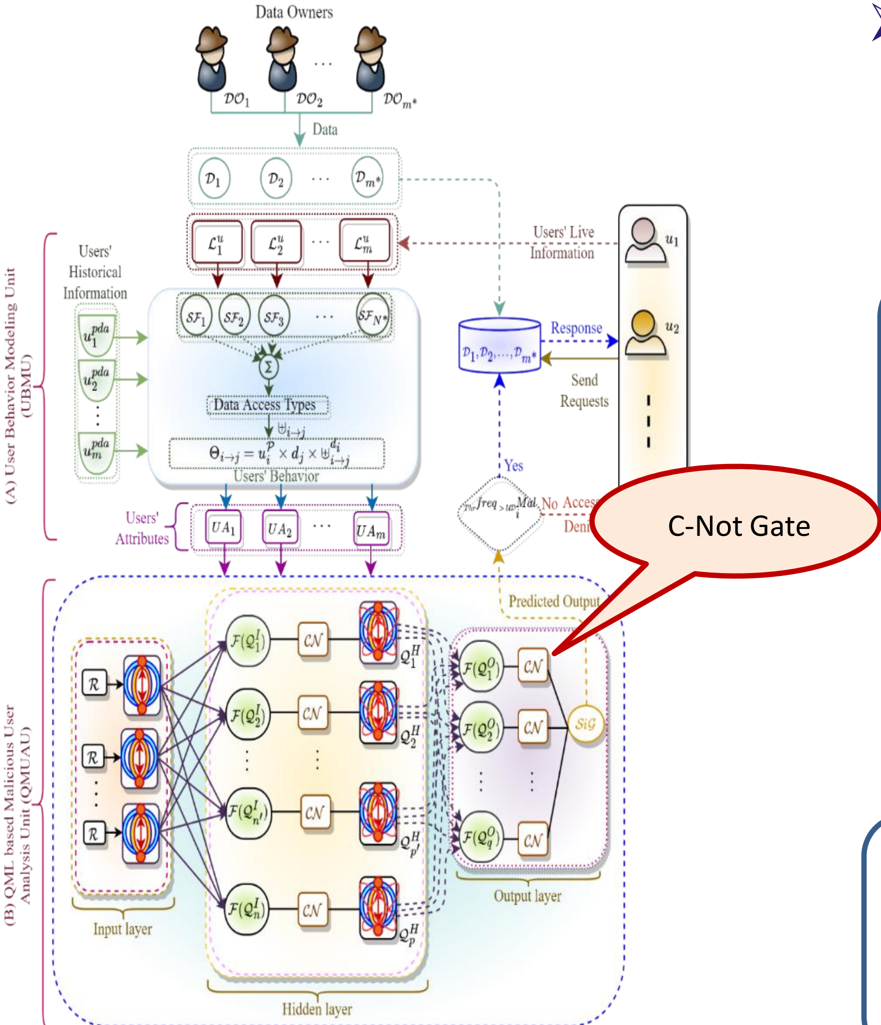
✓ At Hidden layer, Qubit vector is obtained by applying C-Not gate effect as an activation function

$$Q_j^H = \frac{\pi}{2} \times \mathcal{G}(\delta^H) - arg(Q^{*H}_j)$$

$$Q^{*H} = \sum_{i=1,j=1}^{n,p} \mathcal{F}(\varpi_{ij}^I) \times \mathcal{F}(Q_i^I) - \mathcal{F}(\mathcal{B}^I)$$

ϖ : *Qubit weight* $\mathcal{B}^I$: *Bias* $\mathcal{G}(\delta^H)$: *Sigmoid function* $arg(Q^{*H}_j)$: *Amplitude of qubit vector*

Proposed Model



➢ QNN Information Processing

✓ At Hidden layer, Qubit vector is obtained by applying C-Not gate effect as an activation function

$$Q_j^H = \frac{\pi}{2} \times \mathcal{G}(\delta^H) - arg(Q^{*H}_j)$$

$$Q^{*H} = \sum_{i=1,j=1}^{n,p} \mathcal{F}(\varpi_{ij}^I) \times \mathcal{F}(Q_i^I) - \mathcal{F}(\mathcal{B}^I)$$

✓ At Output layer, predicted output is obtained by applying C-Not gate effect and sigmoid function as an activation function

$$y^O = \frac{\pi}{2} \times \mathcal{G}(\delta^O) - arg(Q^{*O})$$

$$Q^{*O} = \sum_{i=1}^{p} \mathcal{F}(\varpi_i^H) \times \mathcal{F}(Q_i^H)$$

ϖ : *Qubit weight* $\mathcal{B}^I$: *Bias* $\mathcal{G}(\delta^H)$: *Sigmoid function* $arg(Q^{*H}_j)$: *Amplitude of qubit vector*

QM-MUP: Operational Summary

Algorithm 1: QM-MUP: Operational Summary

Parameters initialization

```
Initialize: list of users (List_U) with related attributes
  and data requests;
Train and re-train DE-QNN with historical and latest
  malicious user data samples, periodically;
for each time-interval {t_a, t_b} do
    for each user (u_i : i ∈ {1, 2, ..., m}) do
        Receive users requests and analyse
          SF={SF_1 ∪ SF_2 ∪ ... ∪ SF_N*} ;
        Examine the probable purpose of data request
          by computing Eq. (12) ;
        Θ^Mal ⇐ DE-QNN(Θ,{L^u_1, L^u_2, ..., L^u_m}) ;
        if Θ^Mal > 0 then
            u_i is 'Malicious' and data access is denied;
        else
            Access is allowed and data is distributed;
        end
    end
end
```

QM-MUP: Operational Summary

Algorithm 1: QM-MUP: Operational Summary

Parameters initialization

Initialize: list of users ($List_{\mathcal{U}}$) with related attributes and data requests;
Train and re-train DE-QNN with historical and latest malicious user data samples, periodically;
for *each time-interval* $\{t_a, t_b\}$ **do**
  for *each user* ($u_i : i \in \{1, 2, ..., m\}$) **do**

User Behavior Modeling Unit

    Receive users requests and analyse $\mathcal{SF}=\{\mathcal{SF}_1 \cup \mathcal{SF}_2 \cup \ldots \cup \mathcal{SF}_{N^*}\}$;
    Examine the probable purpose of data request by computing Eq. (12) ;
    $\Theta^{Mal} \Leftarrow$ DE-QNN($\Theta, \{\mathcal{L}_1^u, \mathcal{L}_2^u, ..., \mathcal{L}_m^u\}$) ;
    if $\Theta^{Mal} > 0$ **then**
      u_i is 'Malicious' and data access is denied;
    else
      Access is allowed and data is distributed;
    end
  end
end

QM-MUP: Operational Summary

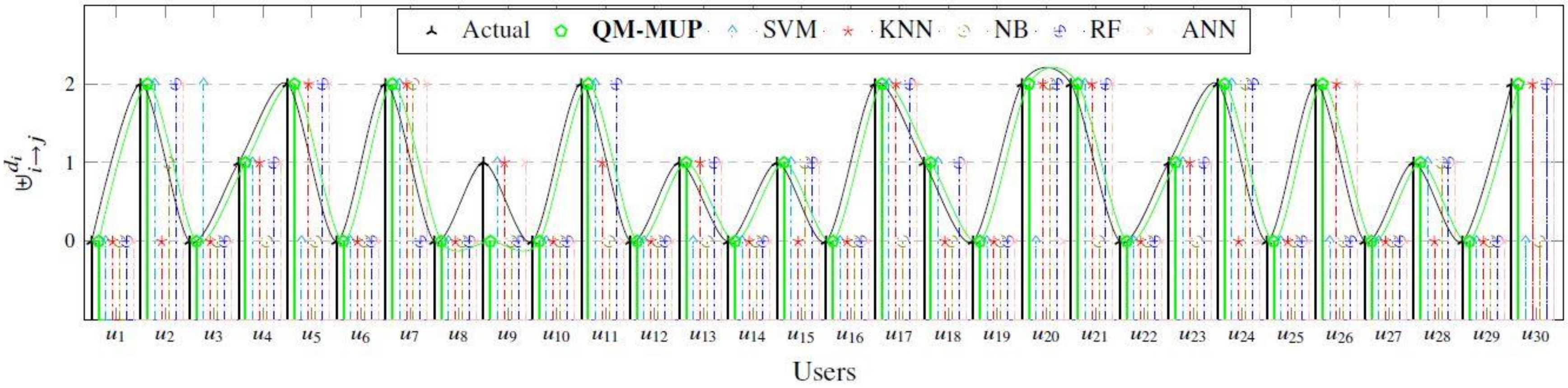
Algorithm 1: QM-MUP: Operational Summary

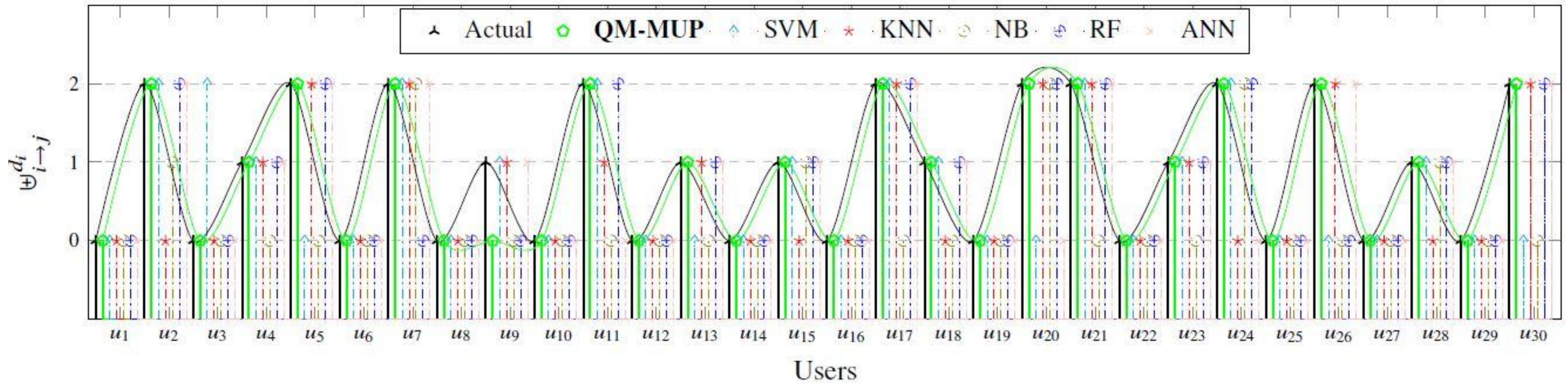
```
Initialize: list of users (List_U) with related attributes
  and data requests;
Train and re-train DE-QNN with historical and latest
  malicious user data samples, periodically;
for each time-interval {t_a, t_b} do
    for each user (u_i : i ∈ {1, 2, ..., m}) do
        Receive users requests and analyse
         SF={SF_1 ∪ SF_2 ∪ ... ∪ SF_N*} ;
        Examine the probable purpose of data request
         by computing Eq. (12) ;
        Θ^Mal ⇐ DE-QNN(Θ,{L_1^u, L_2^u, ..., L_m^u}) ;
        if Θ^Mal > 0 then
            u_i is 'Malicious' and data access is denied;
        else
            Access is allowed and data is distributed;
        end
    end
end
```

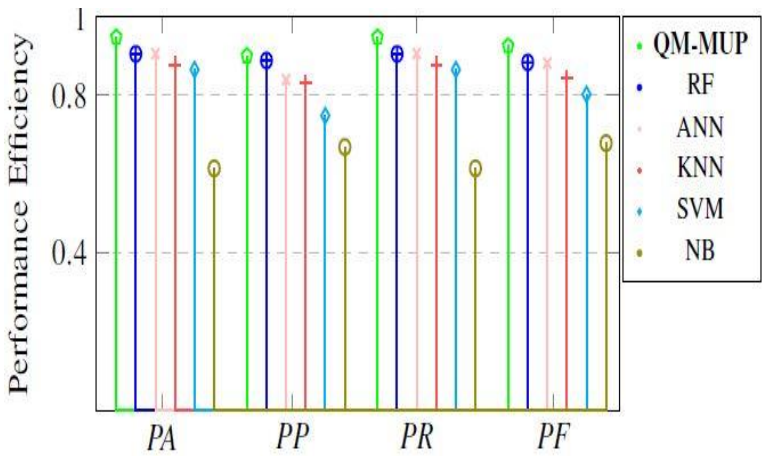
Parameters initialization

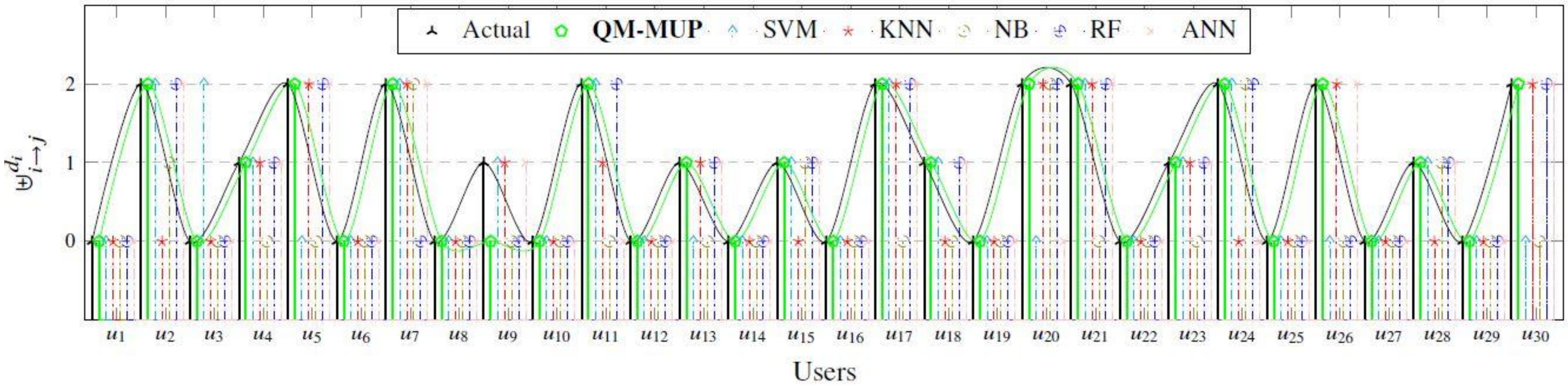
User Behavior Modeling Unit

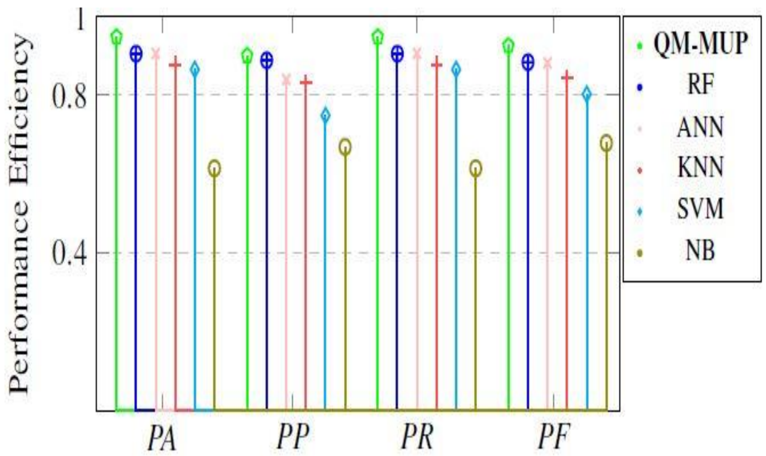
QML based Malicious User Analysis Unit

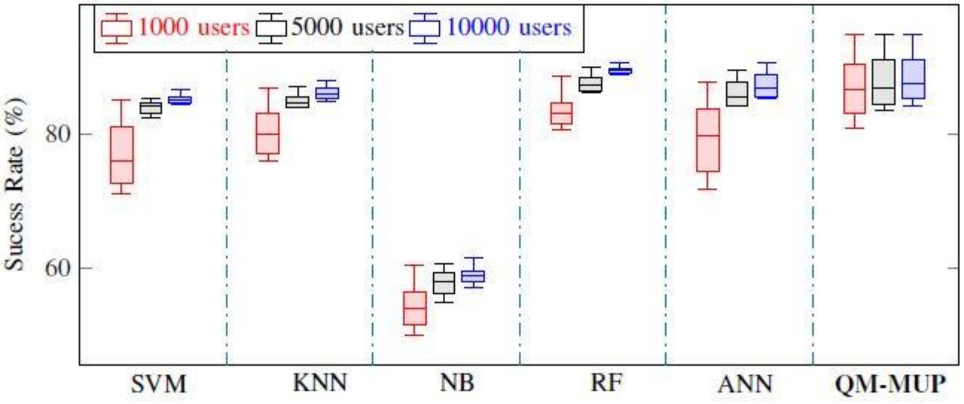

Actual
QM-MUP
SVM
KNN
NB
RF
ANN
2
1
0
$\Theta_{i \to j}^{d_i}$
u_1 u_2 u_3 u_4 u_5 u_6 u_7 u_8 u_9 u_{10} u_{11} u_{12} u_{13} u_{14} u_{15} u_{16} u_{17} u_{18} u_{19} u_{20} u_{21} u_{22} u_{23} u_{24} u_{25} u_{26} u_{27} u_{28} u_{29} u_{30}
Users

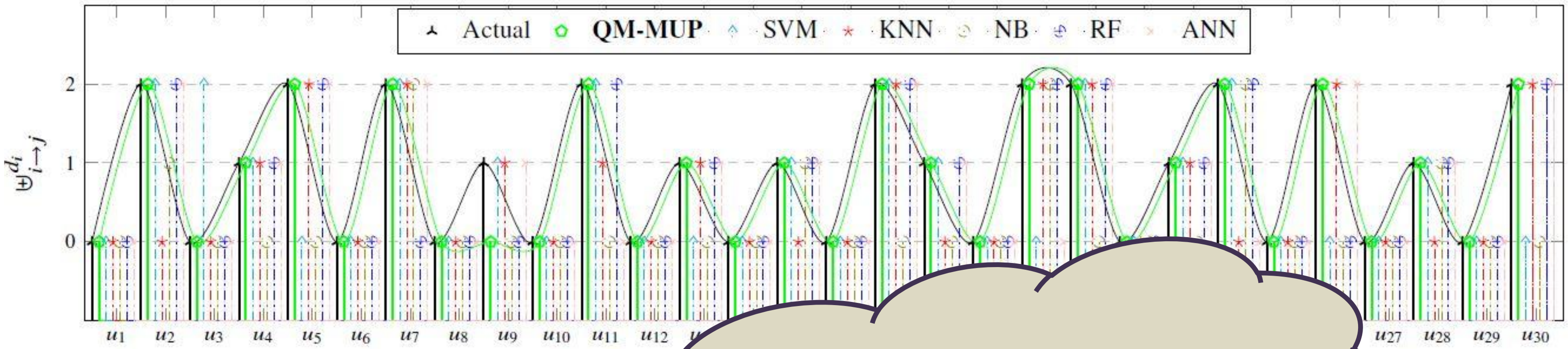

Actual
QM-MUP
SVM
KNN
NB
RF
ANN
$\Theta_{i \to j}^{d_i}$
2
1
0
u_1 u_2 u_3 u_4 u_5 u_6 u_7 u_8 u_9 u_{10} u_{11} u_{12} u_{13} u_{14} u_{15} u_{16} u_{17} u_{18} u_{19} u_{20} u_{21} u_{22} u_{23} u_{24} u_{25} u_{26} u_{27} u_{28} u_{29} u_{30}
Users


Performance Efficiency
1
0.8
0.4
PA
PP
PR
PF
QM-MUP
RF
ANN
KNN
SVM
NB

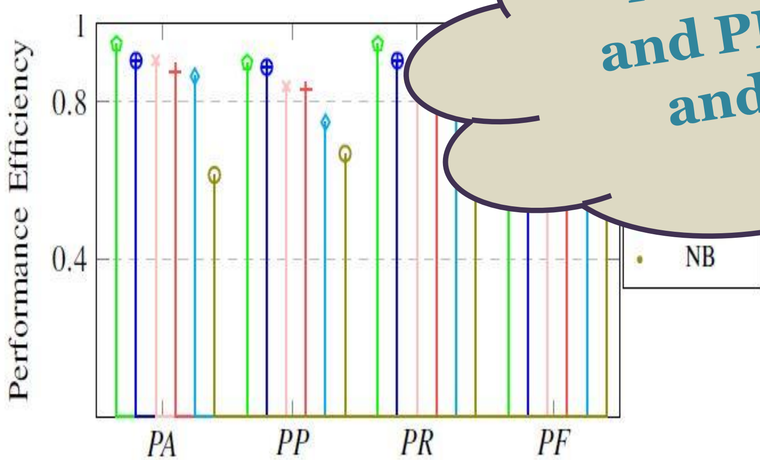

Actual
QM-MUP
SVM
KNN
NB
RF
ANN
Users

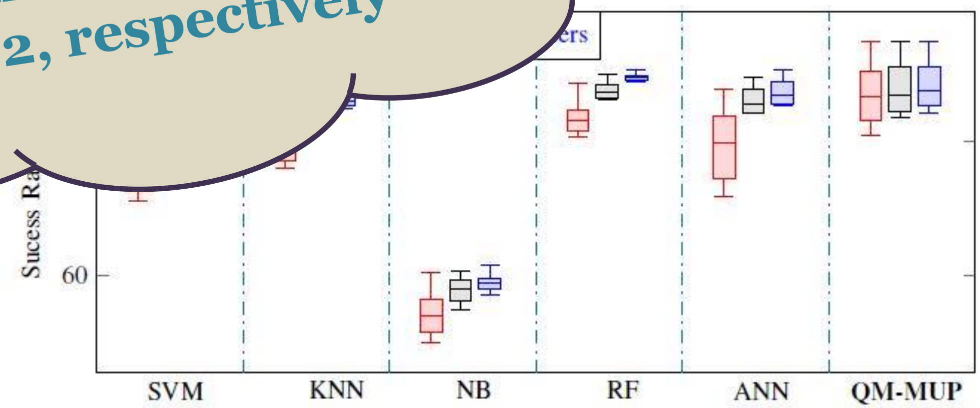

Performance Efficiency
QM-MUP
RF
ANN
KNN
SVM
NB
PA
PP
PR
PF

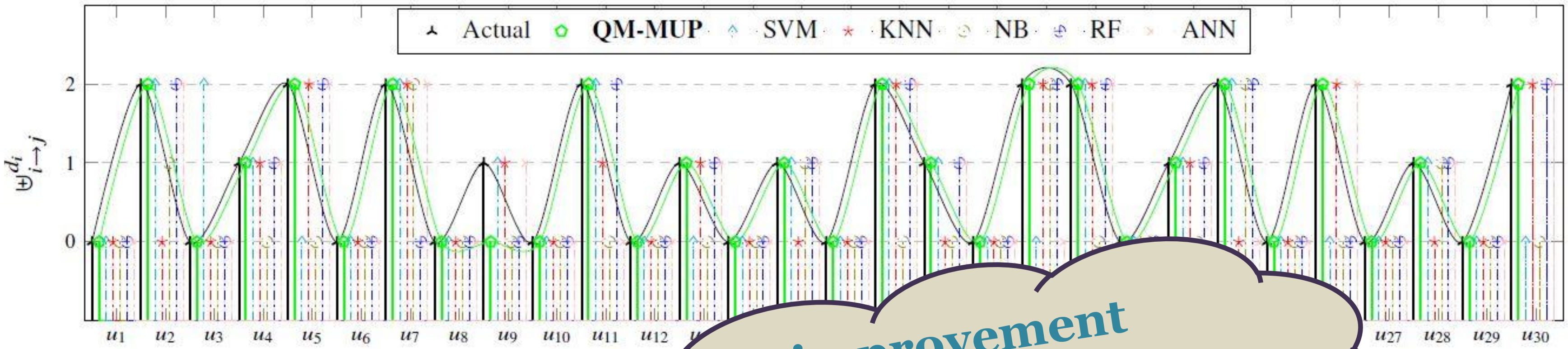

1000 users
5000 users
10000 users
Sucess Rate (%)
SVM
KNN
NB
RF
ANN
QM-MUP



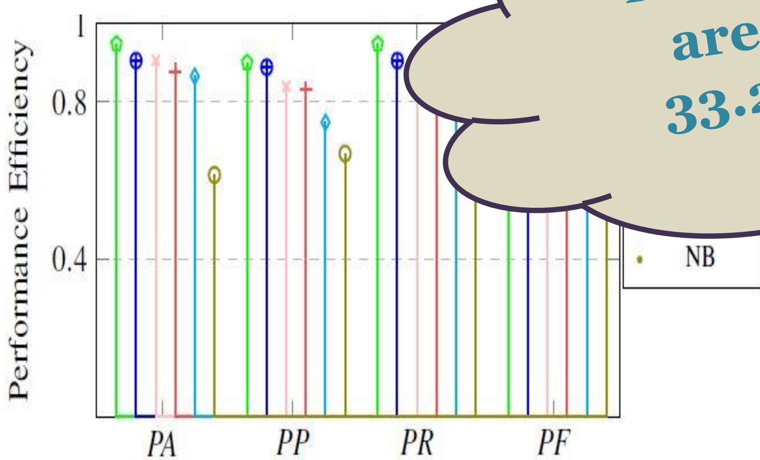
Maximum PA, PP, PR, and PF are 94%, .90, .94, and .92, respectively

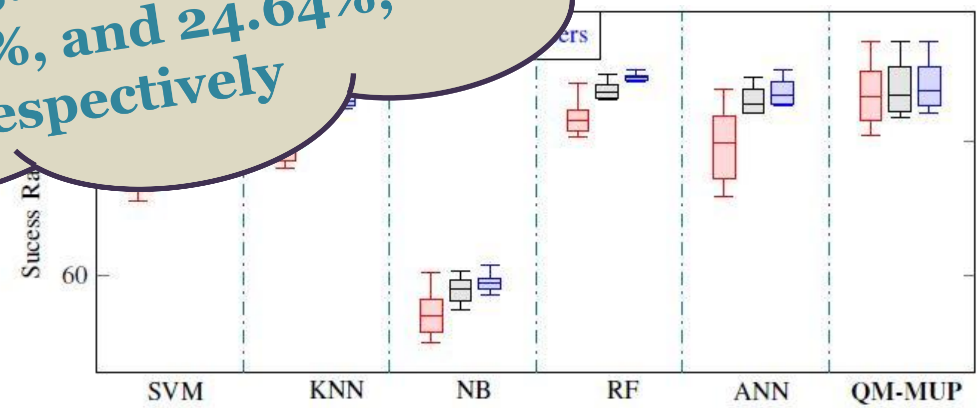






Maximum improvement for PA, PP, PR, and PF are 33.28%, 23.11%, 33.28%, and 24.64%, respectively





Summary

- The different newly proposed secure data protection model, such as DT-PPM, are capable of improving data and its communication security while maintaining utility and reducing computation time.

- QM-MUP avoid data breaches due to malicious, non-malicious, and unknown users and substantially decrease intended cyberthreats.

Future Research Plans

- To develop cybersecurity models seeking proactive cyber threat detection by applying Quantum Machine Learning approaches for secure data communications

- To upgrade data protection by engaging effective privacy mechanisms and facilitate automatic optimization of the accuracy of query results while maintaining security

- To implement the newly proposed models in a simulated distributed computing environment for maximizing the security of user stored and shared data

References

1) Zaghloul, E., Zhou, K., & Ren, J. (2019). P-mod: Secure privilege-based multilevel organizational data-sharing in cloud computing. IEEE Transactions on Big Data.
2) Xu, S., Yang, G., Mu, Y., & Deng, R. H. (2018). Secure fine-grained access control and data sharing for dynamic groups in the cloud. IEEE Transactions on Information Forensics and Security, 13(8), 2101-2113.
3) Li, P., Li, T., Ye, H., Li, J., Chen, X., & Xiang, Y. (2018). Privacy-preserving machine learning with multiple data providers. Future Generation Computer Systems, 87, 341-350.
4) Ma, X., Ma, J., Li, H., Jiang, Q., & Gao, S. (2021). PDLM: Privacy-preserving deep learning model on cloud with multiple keys. IEEE Transactions on Services Computing.
5) Gupta, I., Gupta, R., Singh, A. K., & Buyya, R. (2021). MLPAM: A machine learning and probabilistic analysis-based model for preserving security and privacy in cloud environment. IEEE Systems Journal, 15(3), 4248-4259.
6) Ali, M., Dhamotharan, R., Khan, E., Khan, S. U., Vasilakos, A. V., Li, K., & Zomaya, A. Y. (2015). SeDaSC: secure data sharing in clouds. IEEE Systems Journal, 11(2), 395-404.

References

7) Fu, Z., Xia, L., Sun, X., Liu, A. X., & Xie, G. (2018). Semantic-aware searching over encrypted data for cloud computing. IEEE Transactions on Information Forensics and Security, 13(9), 2359-2371.
8) Casino, F., Domingo-Ferrer, J., Patsakis, C., Puig, D., & Solanas, A. (2015). A k-anonymous approach to privacy preserving collaborative filtering. Journal of Computer and System Sciences, 81(6), 1000-1011.
9) Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006, March). Calibrating noise to sensitivity in private data analysis. In Theory of cryptography conference (pp. 265-284). Springer, Berlin, Heidelberg.
10) Tanuwidjaja, H. C., Choi, R., Baek, S., & Kim, K. (2020). Privacy-Preserving Deep Learning on Machine Learning as a Service-a- Comprehensive Survey. IEEE Access, 8, 167425-167447.
11) Kouda, N., Matsui, N. and Nishimura, H., 2004. A multilayered feed-forward network based on qubit neuron model. *Systems and Computers in Japan*, *35*(13), pp.43-51.
12) Xu, Y., Wang, L., Wang, C., & Zhu, H. (2022). Effective Agent Quantum Private Data Query against Malicious Joint Attack with Blind Quantum Computing. International Journal of Theoretical Physics, 61(4), 1-13.


Thank you