# **Revamping Federated Learning Security from a Defender's Perspective: A Unified Defense with** Homomorphic Encrypted Data Space K Naveen Kumar, Reshmi Mitra, and C Krishna Mohan

### **Federated Learning (FL)**

- A distributed machine learning framework with a central server and *n* clients
- Central server makes use of computational resources of clients, without the need to collect their data
- Data remain on the clients and only model parameters are exchanged ensuring privacy

### Threats models (TM) in our FL setup (Fig. 1)

- Source: Honest-but-curious (HbC) central server
- **Knowledge:** Black-box
- TM1 (utility-centric): Untargeted evasion data poisoning attack
- TM2 (privacy-centric): Model inversion attack (MIA)
- Capabilities: No access to clients' data, model updates, aggregation algorithm, and shared-secret key TM1: utility-centred



## Fig 1. Overview of two different threat models (TM) with potential vulnerabilities and attacks during inference.

### Federated cryptography defense (FCD)



Fig 2. Proposed row-wise symmetric transposition cipher-based FCD transformation

cs19m20p00001@iith.ac.in, rmitra@semo.edu, and ckm@cse.iith.ac.in





TM2: privacy-centred

private data



$\leftarrow$ Secret key $\mathcal{K}$ shared by the server											Algorithm 1 Standard FL with our FCD framework					
Client-side trans $x_1$ $x_2$ $x_3$ $x_4$ $x_4$ $x_5$ $x_5$ $x_7$	ining <b>D</b> encrypted $(\mathcal{E}(\mathcal{X}) = \mathcal{R}_{\mathcal{K}})$ $\mathcal{E}(x_1) = \mathcal{E}(x_2)$ oilities f the FCD-in- entropy loss between the e losses colled ted time com- er of sample ted time sive Total clients, n us 3 5	► Local teacher m input data space $(\mathcal{X}^{T}), \mathcal{Y})$ Local m $(\mathcal{X}^{3})$ → $\mathcal{Y}$ Integrated FL s as $\mathcal{L}_{CE}$ for the e pretrained teacher the e pretrained teacher the e pretrained teacher the space of the sectively update space of the sectively updates sectively of our as and $h$ denounds client updates sed per round, $m$	ecret key $\chi$ sha lodel $\mathcal{P}$ model $\mathcal{P}$ model $\mathcal{P}$ $\mathcal{P}$ model $\mathcal{P}$ $\mathcal$	$ = \int_{c} \mathcal{L}_{ce}(f_{\theta}) $ $ = \int_{ce} \mathcal{L}_{ce}(f_{\theta}) $	server $\kappa_L(Q, \mathcal{P})$ $\downarrow$ $\sigma(\mathcal{E}(\mathcal{X}), \mathcal{Y})$ $\downarrow$ $\mathcal{C}_{CE} + \alpha \mathcal{L}$ $\mathcal{L}$	KL   KL <th>Aggregated obal model <math>G_{\theta}</math> <math>X_{test}</math> <math>X_{test}</math> <math>X_{test}</math> <math>X_{test}</math> <math>X_{test}</math> R R R R R R R R R R</th> <th>Server-s Server-s <math>= \mathcal{E}(\hat{\mathcal{X}}_{test})</math> econstructed and serve the distil normal a ansformal ansformal fically <math>\mathcal{O}</math></th> <th>side exec M M M M M M M M M M M M M M M M M M M</th> <th>cution [alicious i [alicious i ] <math>\oplus</math> <math>\hat{\chi}_{te}</math> <math>\hat{\chi}_{te}</math> <b>Speed limit</b> el inversi data <math>\hat{\chi}_{te}</math> <b>Speed limit</b> el inversi data <math>\hat{\chi}_{te}</math> <b>Speed limit</b> el inversi data <math>\hat{\chi}_{te}</math></th> <th>nference Gradient noise TM1 80 (93%) on attack TM2 n. We ng KL data, ypted</th> <th>Input:GlobaOutput:GlobaOutput:Globa1:Client exa2:for each c3:Train4:<math>\{\mathcal{P}_{i,k}\}</math>5:<math>\mathcal{E}(\mathcal{X}_k) \leftarrow</math>6:for each c7:Initial8:for b =9:<math>\{\mathcal{Q}_k\}</math>10:<math>\mathcal{L}_{0}</math>11:<math>\mathcal{L}_{0}</math>12:<math>\mathcal{L}_{k}</math>13:<math>\theta_k^t</math>14:<math>\nabla \theta_k^t \notin</math>15:return16:Server ex17:Share <math>\theta_g^t</math>,18:Receive m19:Perform m20:Update the21:<math>\hat{\mathcal{X}_{test} \leftarrow \mathbf{I}</math>22:<math>\mathcal{E}(\hat{\mathcal{X}_{test}) \leftarrow \mathbf{I}</math>23:Compute24:return <math>\mathcal{A}_g</math></th> <th>I model <math>\mathcal{G}_{\theta,t}</math>, local bal test accuracy <math>\mathcal{F}_{e}</math> cution <math>(\theta_{g}^{t}, \mathcal{K})</math>: lient <math>k = 1</math> to <math>n \in</math> teacher model <math>\mathcal{F}_{i} = (1, \mathcal{N}_{k}) \leftarrow \{\sigma(x), \mathcal{K}\}</math> lient <math>k = 1</math> to <math>n \in</math> ize the local model <math>z = 1</math> to batches <math>\in</math> <math>\mathcal{D}_{b,k} \} \leftarrow \{\sigma(f_{\theta,0})\}</math> <math>\mathcal{L}_{b,k} \{\mathcal{Q}_{b,k}, \mathcal{Y}_{b,k}\} \leftarrow \{\sigma(f_{\theta,0})\}</math> <math>\mathcal{L}_{b,k} \{\mathcal{Q}_{b,k}, \mathcal{Y}_{b,k}\}</math> <math>\mathcal{L}_{cE_{k}} (\mathcal{Q}_{b,k}, \mathcal{Y}_{b,k}) \leftarrow \{\sigma(f_{\theta,0})\}</math> <math>\mathcal{L}_{b,k} \{\mathcal{Q}_{b,k}, \mathcal{Y}_{b,k}\}</math> <math>\mathcal{L}_{cE_{k}} (\mathcal{Q}_{b,k}, \mathcal{Y}_{b,k})</math> <math>\mathcal{L}_{cE_{k}} (\mathcal{L}_{cE_{k}}, \mathcal{L}_{cE_{k}})</math> <math>\mathcal{L}_{cE_{k}} (\mathcal{L}_{cE_{k}}, \mathcal{L}_{cE_{k}})</math> <math>\mathcal{L}_{cE_{k}} (\mathcal{L}_{cE_{k}})</math> <math>\mathcal{L}_{cE_{k}} (\mathcal{L}_{cE_{k}})</math> <math>\mathcal{L}_{cE_{k}} (\mathcal{L}_{cE_{k}})</math> <math>\mathcal{L}_{cE_{k}} (\mathcal{L}_{cE_{k}})</math> <math>\mathcal{L}_{cE_{k}} (\mathcal{L}_{cE_{k}})</math> <math>\mathcal{L}_{cE_{k}} (\mathcal{L}_{cE_{k}})</math> <math>\mathcal{L}_{cE_{k}} (\mathcal{L}_{cE_{k}})</math> <math>\mathcal{L}_{cE</math></th> <th><math display="block">\frac{1}{d} \operatorname{data} \mathcal{D}_{k} = \mathcal{A}_{g}</math> <math display="block">\frac{1}{d} \operatorname{data} \mathcal{D}_{k} = \operatorname{norm} \mathcal{A}_{g}</math> <math display="block">\frac{1}{d} \operatorname{data} \mathcal{D}_{k} = \operatorname{norm} \mathcal{A}_{g}</math> <math display="block">\frac{1}{d} \operatorname{data} \mathcal{D}_{k} = \mathcal{A}_{g}</math> <math display="block">\frac{1}{d} \operatorname{data} = \mathcal{A}_{g}</math> <math display="block">\frac{1}{</math></th> <th><math>(\mathcal{X}_k, \mathcal{Y}_k)</math> al data <math>\mathcal{D}_k</math> =(1,<math>\mathcal{N}_k</math>) ss-entropy istillation let tal loss (Eq. b TM1, T )</th> <th>loss oss <math>\mathbf{I}</math>. <math><b>4</b></math>)</th>	Aggregated obal model $G_{\theta}$ $X_{test}$ $X_{test}$ $X_{test}$ $X_{test}$ $X_{test}$ R R R R R R R R R R	Server-s Server-s $= \mathcal{E}(\hat{\mathcal{X}}_{test})$ econstructed and serve the distil normal a ansformal ansformal fically $\mathcal{O}$	side exec M M M M M M M M M M M M M M M M M M M	cution [alicious i [alicious i ] $\oplus$ $\hat{\chi}_{te}$ $\hat{\chi}_{te}$ <b>Speed limit</b> el inversi data $\hat{\chi}_{te}$ <b>Speed limit</b> el inversi data $\hat{\chi}_{te}$ <b>Speed limit</b> el inversi data $\hat{\chi}_{te}$	nference Gradient noise TM1 80 (93%) on attack TM2 n. We ng KL data, ypted	Input:GlobaOutput:GlobaOutput:Globa1:Client exa2:for each c3:Train4: $\{\mathcal{P}_{i,k}\}$ 5: $\mathcal{E}(\mathcal{X}_k) \leftarrow$ 6:for each c7:Initial8:for b =9: $\{\mathcal{Q}_k\}$ 10: $\mathcal{L}_{0}$ 11: $\mathcal{L}_{0}$ 12: $\mathcal{L}_{k}$ 13: $\theta_k^t$ 14: $\nabla \theta_k^t \notin$ 15:return16:Server ex17:Share $\theta_g^t$ ,18:Receive m19:Perform m20:Update the21: $\hat{\mathcal{X}_{test} \leftarrow \mathbf{I}$ 22: $\mathcal{E}(\hat{\mathcal{X}_{test}) \leftarrow \mathbf{I}$ 23:Compute24:return $\mathcal{A}_g$	I model $\mathcal{G}_{\theta,t}$ , local bal test accuracy $\mathcal{F}_{e}$ cution $(\theta_{g}^{t}, \mathcal{K})$ : lient $k = 1$ to $n \in$ teacher model $\mathcal{F}_{i} = (1, \mathcal{N}_{k}) \leftarrow \{\sigma(x), \mathcal{K}\}$ lient $k = 1$ to $n \in$ ize the local model $z = 1$ to batches $\in$ $\mathcal{D}_{b,k} \} \leftarrow \{\sigma(f_{\theta,0})\}$ $\mathcal{L}_{b,k} \{\mathcal{Q}_{b,k}, \mathcal{Y}_{b,k}\} \leftarrow \{\sigma(f_{\theta,0})\}$ $\mathcal{L}_{b,k} \{\mathcal{Q}_{b,k}, \mathcal{Y}_{b,k}\}$ $\mathcal{L}_{cE_{k}} (\mathcal{Q}_{b,k}, \mathcal{Y}_{b,k}) \leftarrow \{\sigma(f_{\theta,0})\}$ $\mathcal{L}_{b,k} \{\mathcal{Q}_{b,k}, \mathcal{Y}_{b,k}\}$ $\mathcal{L}_{cE_{k}} (\mathcal{Q}_{b,k}, \mathcal{Y}_{b,k})$ $\mathcal{L}_{cE_{k}} (\mathcal{L}_{cE_{k}}, \mathcal{L}_{cE_{k}})$ $\mathcal{L}_{cE_{k}} (\mathcal{L}_{cE_{k}}, \mathcal{L}_{cE_{k}})$ $\mathcal{L}_{cE_{k}} (\mathcal{L}_{cE_{k}})$ $\mathcal{L}_{cE_{k}} (\mathcal{L}_{cE_{k}})$ $\mathcal{L}_{cE_{k}} (\mathcal{L}_{cE_{k}})$ $\mathcal{L}_{cE_{k}} (\mathcal{L}_{cE_{k}})$ $\mathcal{L}_{cE_{k}} (\mathcal{L}_{cE_{k}})$ $\mathcal{L}_{cE_{k}} (\mathcal{L}_{cE_{k}})$ $\mathcal{L}_{cE_{k}} (\mathcal{L}_{cE_{k}})$ $\mathcal{L}_{cE$	$\frac{1}{d} \operatorname{data} \mathcal{D}_{k} = \mathcal{A}_{g}$ $\frac{1}{d} \operatorname{data} \mathcal{D}_{k} = \operatorname{norm} \mathcal{A}_{g}$ $\frac{1}{d} \operatorname{data} \mathcal{D}_{k} = \operatorname{norm} \mathcal{A}_{g}$ $\frac{1}{d} \operatorname{data} \mathcal{D}_{k} = \mathcal{A}_{g}$ $\frac{1}{d} \operatorname{data} = \mathcal{A}_{g}$ $\frac{1}{$	$(\mathcal{X}_k, \mathcal{Y}_k)$ al data $\mathcal{D}_k$ =(1, $\mathcal{N}_k$ ) ss-entropy istillation let tal loss (Eq. b TM1, T )	loss oss $\mathbf{I}$ . $4$ )
GTSRB [61]         TM1         KBTS [40]         CIFAR10 [30]         EMNIST [9]	3, 5, 10, 15, 25 100 10000	3, 5, 10, 15, 25 40 and 70 100 and 500	- 30, 50, and	1100	Custon CNN ResNet18 LeNet5	m [ [21] [34]	200 500	5 10	0.1, 0.5 (de 1	0.2, efault), U , 5,	$= \mathcal{A}_g - \mathcal{A}_g^*$		Speed limit 80 (95.2%) (93.	cial Pedestrian ance crossing 8%) (94.9%)	No entry (95.3%)	Yield (94.8%)
TM2 CIFAR100 [30]	Exact setup use	d in [35], $n = m = 2$	( <del>**</del>		VGG11	[59]	200	1	2	2	MSE	Original data	80			
Table 2. Comparison of evasion defenses in terms of impact on utility (U) ↓ under M-SimBA attack across different         FL configurations. ND denotes an FL system without defense. Bold indicate best results.												M-SimBA attack data (human eye imperceivable perturbations)	Stop (90.7%)Overt (89.Image: Stop (90.7%)Image: Stop (89.	aking       Bicycle cross         4%)       (92.9%)         Image: Comparison of the second secon	Ing Speed Speed Speed Speed Speed Speed (91.6%)	Deer crossing (89.8%)
<b>Dataset</b> Setting $\frac{A_1}{n}$	$p \rightarrow m = m$ ND	FAT [81] RS [10	1 FCD (ours)	ND	FAT [81]	RS [10]	FCD (ours)	ND	FAT [81]	RS [10]	FCD (ours)					
Hom GTSRB [61] Het	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$\begin{array}{cccc} 0.52 \pm 0.73 \\ 0.71 \pm 1.32 \\ 0.91 \pm 1.04 \\ 2 & 2.84 \pm 0.70 \\ 3 & 6.62 \pm 0.68 \\ 1 & 0.23 \pm 0.19 \\ 5 & 1.78 \pm 1.09 \\ 9 & 5.82 \pm 0.93 \\ 9 & 0.96 \pm 1.53 \\ 73 & 8.08 \pm 0.11 \end{array}$	$50.05 \pm 1.34$ $58.25 \pm 1.41$ $73.45 \pm 0.41$ $72.65 \pm 1.84$ $79.95 \pm 1.05$ $56.58 \pm 1.15$ $64.28 \pm 1.81$ $69.28 \pm 1.54$ $74.58 \pm 0.76$ $76.98 \pm 0.35$	$\begin{array}{c} 1.35 \pm 1.11 \\ 1.43 \pm 1.47 \\ 4.64 \pm 0.43 \\ 9.95 \pm 1.18 \\ 13.47 \pm 0.97 \\ \hline 0.86 \pm 0.66 \\ 4.39 \pm 1.42 \\ 3.76 \pm 1.65 \\ 8.62 \pm 0.19 \\ 15.11 \pm 0.92 \end{array}$	$\begin{array}{c} 0.43 \pm 1.90 \\ 1.83 \pm 1.50 \\ 4.3 \pm 1.85 \\ 5.94 \pm 1.87 \\ 14.48 \pm 1.62 \\ 0.15 \pm 1.05 \\ 2.38 \pm 0.58 \\ 7.29 \pm 1.52 \\ 10.21 \pm 0.93 \\ 23.61 \pm 0.15 \end{array}$	$\begin{array}{c} 0.27 \pm 1.12 \\ 1.01 \pm 0.87 \\ 3.12 \pm 0.84 \\ 4.13 \pm 1.38 \\ 7.92 \pm 1.39 \\ \hline{0.10 \pm 0.77} \\ 1.41 \pm 0.26 \\ \hline{1.81 \pm 1.43} \\ 6.33 \pm 0.73 \\ 9.28 \pm 1.79 \end{array}$	$\begin{array}{c} 53.25 \pm 1.10 \\ 64.25 \pm 1.83 \\ 79.35 \pm 1.80 \\ 75.25 \pm 1.17 \\ 81.55 \pm 0.67 \\ 59.48 \pm 1.53 \\ 64.68 \pm 0.59 \\ 73.78 \pm 1.62 \\ 75.38 \pm 1.18 \\ 77.08 \pm 1.32 \end{array}$	$1.92 \pm 1.16$ $3.01 \pm 0.34$ $7.88 \pm 1.13$ $11.81 \pm 1.25$ $17.12 \pm 0.94$ $1.03 \pm 1.36$ $3.38 \pm 1.64$ $9.72 \pm 1.15$ $11.92 \pm 1.57$ $18.86 \pm 1.93$	$\begin{array}{c} 1.74 \pm 1.23 \\ 2.32 \pm 1.61 \\ 5.93 \pm 1.31 \\ 7.83 \pm 1.03 \\ 11.3 \pm 0.27 \\ 0.96 \pm 1.70 \\ 4.59 \pm 1.86 \\ 7.39 \pm 0.98 \\ 13.15 \pm 1.72 \\ 24.86 \pm 1.30 \end{array}$	$\begin{array}{c} 0.85 \pm 0.99 \\ 1.27 \pm 1.59 \\ 4.41 \pm 1.72 \\ 5.2 \pm 1.25 \\ 9.02 \pm 0.61 \\ 0.22 \pm 0.75 \\ 2.9 \pm 0.97 \\ 5.52 \pm 0.36 \\ 9.28 \pm 1.01 \\ 11.58 \pm 0.17 \end{array}$	FCD encrypted data Fig 3. Vi M-SimBA GTSRB d	version versio	<ul> <li>ial nace 4%)</li> <li>ial crossing (93.7%)</li> <li>iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii</li></ul>	No entry (93.9%) IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Yield (92.8%) Monte of the second sec
cce iith ac in										Con	nect wit	h me on	TinkedT	n•		

$\blacksquare$ Secret key $\mathcal{K}$ shared by the server												Algorithm 1 Standard FL with our FCD framework									
Client-side training							Server-side execution								<b>Input:</b> Global model $\mathcal{G}_{\theta,t}$ , local data $\mathcal{D}_k = (\mathcal{X}_k, \mathcal{Y}_k)$						
									1	202		Mal	icious in	ference	Output: G	obal test accu	racy $\mathcal{A}_g$				
$x_1$				Local te	eacher moo		$ \longrightarrow \mathcal{L} $	$_{KL}(\mathcal{Q},\mathcal{P})$	A	ggregated				Gradient	2: for each	client $k = 1$	to n do				
		FCD er	icrypted i	input data	space	$\mathcal{P}$		Ţ	glo	bal model		(80) 6	Ð	noise	3: Tra	in teacher me	del far o	on normal	data Dr.		
$x_2$	Ta	$\langle \mathcal{E}(\mathcal{A}) \rangle$	$\mathcal{C}) = \mathcal{R}_{\mathcal{K}}(\mathcal{C})$	$(\mathcal{X}^{\mathcal{T}}), \mathcal{Y})$	Local mo	del	$\rightarrow f_{ar}(f_{ar})$	$(\mathcal{E}(\mathcal{X}))$	$(\mathbf{v})$	Gθ			$\hat{\chi}_{}$	TM1	4: $\{\mathcal{P}_i\}$	$_{k}_{i=(1,N_{k})} \leftarrow$	{ (fo.k(	$\chi_{i,k}))\}_{i=0}$	1. 1.6.)		
	23							$(c(\alpha), y)$	, , , , ,	* Xtest	$= \mathcal{E}(\hat{\mathcal{X}_{test}})$	<b>*</b>	test		5. E(X.)	- FCD (X. A	0				
<b>Original</b> in	nput		$\mathcal{E}(x_1) \in$	(m)		Q						> Spe	ed limit 80	) (93%)	6: for each	client $k = 1$	to n do				
data spa	ice			$(x_3) - (x_3)$			$\mathcal{L} = \mathcal{L}$	$\mathcal{L}_{CE} + \alpha \mathcal{L}$		₹// +		Model	inversio	n attack	7: Initi	alize the local	model $\theta_k^t$	$\leftarrow \theta_o^t$			
$(\mathcal{X},\mathcal{Y})$		E	$(x_2)$	-											8: for	b = 1 to batch	les $\in \mathcal{E}(\mathcal{X})$	$_{k})$ do			
P.Q.: prediction probabilities Back propagation Reconstructed private data											TM2	9:	$\{Q_{b,k}\} \leftarrow \{\sigma$	$(f_{\theta,0}(\mathcal{E}(\lambda$	$k_{k}[b]))))$						
	-														10:	$\mathcal{L}_{CE_k}(\mathcal{Q}_{b,k}, \mathbf{J})$	$(b,k) \leftarrow E(b,k)$	q. 2, Cross	entropy lo	OSS	
<b>Fig 3.</b> (	Fig 3. Overview of the FCD-integrated FL system, with a focus on one client's training and server-side execution. We														11: $\mathcal{L}_{KLD_k}(\mathcal{Q}_{b,k}    \mathcal{P}_{b,k}) \leftarrow \text{Eq. 3, Distillation loss}$ 12: $\mathcal{L}_{KLD_k}(\mathcal{Q}_{b,k}    \mathcal{P}_{b,k}) \leftarrow \text{Eq. 3, Distillation loss}$						
comput	te the cros	ss-enti	ropy los	s $\mathcal{L}_{CE}$ fo	or the lo	cal model	on encr	vpted da	ata and	calculate	the distil	lation los	s using	gKL	12: $\mathcal{L}_k \leftarrow \mathcal{L}_{CE_k} + \alpha_k \mathcal{L}_{KLD_k} \triangleright \text{ fotal loss (Eq. 4)}$ 13: $\theta_i^t \leftarrow \theta_i^t - n \nabla_{ot} f_{i}$						
diverg	Pence <i>L</i> <sub>K</sub>	r betw	veen the	pretrai	ned teac	eher mode	el and th	e local s	tudent i	model for	normal a	nd encry	nted d	ata.	14. 57.00	, at at	· Ok ~K				
resnect	$\sim_{KL}$ between the prediction of the local model $f_{a}$ Similarly test data is transformed into the energy test														14: $\nabla \theta_k^c \leftarrow \theta_k^c - \theta_g^c$ 15: return $\nabla \theta^t$						
respect					apuare e	ne to com	tor noto	ntial att	oolze					puu	16 Server	execution $(\nabla$	At ).				
					spa			ππάι άτι	acns.						17: Share $\theta$	K to all the	clients				
Lemma	: The expe	ected t	ime com	plexity	of our F	CD encryp	otion fund	ction $\mathcal{E}($	$\mathcal{X}$ ) is lin	near, speci	fically $\mathcal{O}$	(nh), whe	ere n		18: Receive	model update	es from se	lected clier	its $\leftarrow \nabla \theta_i^t$		
represent	ts the num	nber of	sample	s. and $h$	denotes	s the imag	e height.	×							19: Perform	model aggre	gation usin	ng FedAvg	(Eq. 5)		
						0	0								20: Update	the global mo	del param	eter: $\theta_g^{t+1}$			
T	able 1. Co	ompre	hensive	experin	nental d	etails: dat	tasets, m	odels, F	'L setup	, attack c	onfigurat	ion, and	metrics	5.	21: $\hat{\mathcal{X}}_{test} \leftarrow$	Poisoned tes	st data	Þ	TM1, T	M2	
Threat		Tot	al	Client upd	ates A	Attack percer	ntage (%).		_						22: $\mathcal{E}(\mathcal{X}_{test})$	$) \leftarrow \text{FCD}(\mathcal{X}_{t},$	est, K)	a/ 12			
model	Dataset	client	ts, n us	ed per rou	<b>nd</b> , <i>m</i>	$A_p = \frac{\rho}{N_e}$	× 100	Mode	el Glo	bal epochs	Local epoch	$\alpha$	1	Metrics	23: Comput	$e \mathcal{A}_g \leftarrow Tes$	$E(\mathcal{G}_{\theta_g^{t+1}}, \mathcal{G}_{\theta_g^{t+1}})$	$\mathcal{E}(\mathcal{X}_{test}))$			
(	GTSRB [61]	3,	5,	3, 5,		JVIC		Custor	m	200	5	0.1, 0.2	2,		24: return .	$A_g$					
TM1	KBTS [40]	10, 15	5, 25	10, 15, 2	25	30 50 ar	d 100	CNN	ſ	200	5	0.5 (defa	ult), $U =$	$= 4 - 4^*$	30.00	Smood limit	Social	Pedestrian			
C	CIFAR10 [30]	10	0	40 and 7	0	50, 50, u	101	ResNet18	[21]	500	10	1,		s g		80 (95.2%)	distance (93.8%)	crossing (94.9%)	No entry (95.3%)	Yield (94.8%)	
TM2 CI	EMNIST [9]	100	00	100  and  5	000			LeNet5	[34]	200	1	2		MCE						7	
INIZ CI	IFAR100 [30	J Exact	setup used	1 in [55], n	= m = 2			VGGII	[39]	200	1	2		MSE	<b>Original data</b>						
																			C 1	Door	
Tabla		oricor	ofour	ion dof	nana in	torma of i	mnoot o	· · · ↓ · ] · ↓ · ·		nndor N/	Sim <b>D</b> A of	toolzoor	a diff	o voo t	M-SimBA	Stop	Overtaking E	Bicycle crossing	limit 100	crossing	
Table	e 2. Comp	arison	ofevas	sion defe	enses in	terms of i	mpact o	n utility	' (U ) ↓ l	under M-	SimBA at	tack acro	oss diff	erent	M-SimBA attack data (human eye	Stop (90.7%)	Overtaking E (89.4%)	Bicycle crossing (92.9%)	Speed limit 100 (91.6%)	crossing (89.8%)	
Table	e 2. Comp F	arison FL con	of evas	sion defe ions. ND	enses in ) denote	terms of i s an FL sy	mpact o ystem wi	n utility ithout de	(U)↓ı efense.]	ınder M-S Bold indic	SimBA at cate best	tack acro results.	oss diffe	erent	M-SimBA attack data (human eye imperceivable perturbations)	Stop (90.7%)	Overtaking E (89.4%)	Bicycle crossing (92.9%)	Speed limit 100 (91.6%)	crossing (89.8%)	
Table      Dataset	e 2. Comp F	$\frac{arison}{FL con}$	of evas	sion defe ions. ND	enses in ) denote 0%	terms of i s an FL sy	mpact o ystem wi	n utility thout de	$(U) \downarrow i$ efense.	under M-S Bold indic	SimBA at ate best	tack acro results.	oss diffe	erent	M-SimBA attack data (human eye imperceivable perturbations)		Overtaking E (89.4%)	Bicycle crossing (92.9%)	Speed limit 100 (91.6%)	crossing (89.8%)	
Table      Dataset	e 2. Comp F	$\frac{arison}{FL con}$ $\frac{A_p \rightarrow}{n = m}$	of evas	sion defendere ions. NC 3 FAT [81]	enses in b denote 0% RS [10]	terms of i s an FL sy FCD (ours)	mpact o ystem wi	n utility thout do 5 FAT [81]	$(U) \downarrow i$ efense. ] 0% RS [10] 0.43+100	Inder M-S Bold indic FCD (ours)	SimBA at ate best	tack acro tack acro results. 1009 FAT [81] F	<b>5 5 5 5 5 5 5 5 5 5</b>	ECD (ours)	M-SimBA attack data (human eye imperceivable perturbations)	Stop (90.7%)	Overtaking (89.4%)	Bicycle crossing (92.9%)	Speed limit 100 (91.6%)	crossing (89.8%)	
Table	e 2. Comp F	$\begin{array}{c} arison\\ FL con\\ \hline A_p \rightarrow\\ n=m\\ \hline 3\\ 5 \end{array}$	of evas figuration 1000000000000000000000000000000000000	ion defe ions. NC 3 FAT [81] 0.99±0.57 1.17±0.56	enses in ) denote 0% RS [10] 0.94±0.71 1.09±0.29	terms of i s an FL sy FCD (ours) 0.52±0.73 0.71±1.32	mpact o ystem wi ND 50.05±1.34 58.25±1.41	n utility thout do 5 FAT [81] 1.35±1.11 1.43±1.47	$(U) \downarrow i$ efense. ] 0% RS [10] 0.43±1.90 1.83±1.50	Inder M-S Bold indic FCD (ours) 0.27±1.12 1.01±0.87	SimBA at eate best 1 ND 53.25±1.10 64.25±1.83	tack acro esults. 1009 FAT [81] F 1.92±1.16 1 3.01±0.34 2	<b>5 [10]</b> <b>5 [10]</b> <b>5 [10]</b> <b>1</b> <b>5</b> <b>5</b> <b>1</b> <b>1</b> <b>1</b> <b>1</b> <b>1</b> <b>1</b> <b>1</b> <b>1</b>	erent FCD (ours) 0.85±0.99 1.27±1.59	M-SimBA attack data (human eye imperceivable perturbations)	et	Covertaking E (89.4%) Covertaking E Covertaking E Covert	Bicycle crossing (92.9%)	Speed limit 100 (91.6%)	Deer crossing (89.8%)	
Table	e 2. Comp For the setting - Hom	$A_p \rightarrow$ $A_p \rightarrow$ $n = m$ $3$ $5$ $10$	of evas figurati figurati 1.85±0.90	5000 defe 5000 defe 5000 defe 3 3 5000 defe 3 3 5000 defe 3 5000 defe 5000 d	enses in b denote 0% RS [10] 0.94±0.71 1.09±0.29 1.86±0.51	terms of i s an FL sy FCD (ours) 0.52±0.73 0.71±1.32 0.91±1.04	mpact o stem wi 50.05±1.34 58.25±1.41 73.45±0.41	n utility thout do 5 FAT [81] 1.35±1.11 1.43±1.47 4.64±0.43	$(U) \downarrow 1$ efense. 3 0% RS [10] 0.43±1.90 1.83±1.50 4.3±1.85	Inder M-S Bold indic Bold indic FCD (ours) 0.27±1.12 1.01±0.87 3.12±0.84	SimBA at ate best 1 53.25±1.10 64.25±1.83 79.35±1.80	tack acro esults. 1009 FAT [81] F 1.92±1.16 1 3.01±0.34 2 7.88±1.13 5	<b>5 [10]</b> <b>5 [10]</b> <b>5 [10]</b> <b>1</b> <b>5 [10]</b> <b>1</b> <b>5</b> <b>1</b> <b>1</b> <b>1</b> <b>1</b> <b>1</b> <b>1</b> <b>1</b> <b>1</b>	erent FCD (ours) 0.85±0.99 1.27±1.59 4.41±1.72	M-SimBA attack data (human eye imperceivable perturbations) FCD encrypted data	secretare secret	Covertaking (89.4%) (89.4%)	Bicycle crossing (92.9%) IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Speed limit 100 (91.6%) IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Yield (92.8%)	
Dataset	e 2. Comp E Setting -	$\begin{array}{c} arison\\ FL con\\ \hline A_p \rightarrow\\ n=m\\ \hline 3\\ 5\\ 10\\ 15\\ \end{array}$	0 f evas figurati figurati 49.55±1.60 58.15±1.69 71.85±0.90 70.35±1.23	5 <b>ion defe</b> <b>Jons. NE</b> 3 <b>FAT [81]</b> 0.99±0.57 1.17±0.56 2.47±0.62 8.84±1.88	enses in b denote 0% RS [10] 0.94±0.71 1.09±0.29 1.86±0.51 3.77±1.12	terms of i s an FL sy FCD (ours) 0.52±0.73 0.71±1.32 0.91±1.04 2.84±0.70	mpact o stem wi 50.05±1.34 58.25±1.41 73.45±0.41 72.65±1.84	n utility thout do 5 FAT [81] 1.35±1.11 1.43±1.47 4.64±0.43 9.95±1.18	$(U) \downarrow 1$ efense. J 0% RS [10] 0.43±1.90 1.83±1.50 4.3±1.85 5.94±1.87	Inder M-S Bold indic Bold indic 500 (ours) 0.27±1.12 1.01±0.87 3.12±0.84 4.13±1.38	SimBA at ate best i 53.25±1.10 64.25±1.83 79.35±1.80 75.25±1.17	tack acro esults. 1009 FAT [81] F 1.92±1.16 1 3.01±0.34 2 7.88±1.13 5 11.81±1.25 7	5 [10] ] 5 [	erent FCD (ours) 0.85±0.99 1.27±1.59 4.41±1.72 5.2±1.25	M-SimBA attack data (human eye imperceivable perturbations)	v-wise secret- key based insformation franspose franspos	Overtaking (89.4%)   For a state of the second state o	Bicycle crossing (92.9%) Ioiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	Speed limit 100 (91.6%) IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Deer crossing (89.8%) <b>Vield</b> (92.8%)	
Table Dataset	e 2. Comp F Setting -	$A_p \rightarrow$ $A_p \rightarrow$ $n = m$ $3$ $5$ $10$ $15$ $25$	0f evas figurati figurati 10 49.55±1.60 58.15±1.69 71.85±0.90 70.35±1.23 79.55±1.13	5 Constant of the second state of the second s	enses in denote denote 0% <u>RS [10]</u> 0.94±0.71 1.09±0.29 1.86±0.51 3.77±1.12 8.93±1.53	terms of i s an FL sy FCD (ours) 0.52±0.73 0.71±1.32 0.91±1.04 2.84±0.70 6.62±0.68	<b>ND</b> 50.05±1.34 58.25±1.41 73.45±0.41 72.65±1.84 79.95±1.05	n utility thout de 5 FAT [81] 1.35±1.11 1.43±1.47 4.64±0.43 9.95±1.18 13.47±0.97	$(U) \downarrow u$ efense. J 0% RS [10] 0.43±1.90 1.83±1.50 4.3±1.85 5.94±1.87 14.48±1.62	Inder M-S Bold indic Bold indic FCD (ours) 0.27±1.12 1.01±0.87 3.12±0.84 4.13±1.38 7.92±1.39	SimBA at ate best i ND 53.25±1.10 64.25±1.83 79.35±1.80 75.25±1.17 81.55±0.67	$\begin{array}{c} \textbf{tack across}\\ tack $	55 diff 55 [10] 1 74±1.23 .32±1.61 .93±1.31 .83±1.03 1.3±0.27	erent FCD (ours) 0.85±0.99 1.27±1.59 4.41±1.72 5.2±1.25 9.02±0.61	M-SimBA attack data (human eye imperceivable perturbations) FCD encrypted data	Row-wise secret- key based transformation transform	Overtaking (89.4%)Image: Social distance (91.4%)Image: Social distance (91.4%)	Bicycle crossing (92.9%) IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Speed limit 100 (91.6%) IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Deelcrossing(89.8%)Image: Constraint of the second	
Table Dataset	e 2. Comp For the setting -	$\begin{array}{c} arison\\ FL con\\ \hline A_p \rightarrow\\ n=m\\ \hline 3\\ 5\\ 10\\ 15\\ 25\\ \hline 3\\ 5\\ \hline 3\\ 5\\ \hline 3\\ 5\end{array}$	<b>Of evas</b> <b>figurati</b> <b>figurati</b> <b>ND</b> 49.55±1.60 58.15±1.69 71.85±0.90 70.35±1.23 79.55±1.13 56.18±1.93 62.68±1.00	5 5 5 5 5 5 5 5 7 5 7 5 7 5 7 5 7 5 7 5	enses in denote denote 0% <b>RS</b> [10] $0.94\pm0.71$ $1.09\pm0.29$ $1.86\pm0.51$ $3.77\pm1.12$ $8.93\pm1.53$ $0.31\pm0.11$ $3.50\pm1.75$	terms of i s an FL sy FCD (ours) 0.52±0.73 0.71±1.32 0.91±1.04 2.84±0.70 6.62±0.68 0.23±0.19 1.78±1.00	<b>ND</b> 50.05±1.34 58.25±1.41 73.45±0.41 72.65±1.84 79.95±1.05 56.58±1.15 64.28±1.01	n utility thout defined of the second state o	$(U) \downarrow u$ efense. J 0% RS [10] 0.43±1.90 1.83±1.50 4.3±1.85 5.94±1.87 14.48±1.62 0.15±1.05 2 38±0.50	Inder M-S Bold indic Bold indic FCD (ours) 0.27±1.12 1.01±0.87 3.12±0.84 4.13±1.38 7.92±1.39 0.10±0.77 1.41±0.24	SimBA at ate best i 33.25±1.10 64.25±1.83 79.35±1.80 75.25±1.17 81.55±0.67 59.48±1.53 64.68±0.50	tack across         tack across         total tack across <th><b>59</b>±1.96</th> <th>erent FCD (ours) <math>0.85 \pm 0.99</math> <math>1.27 \pm 1.59</math> <math>4.41 \pm 1.72</math> <math>5.2 \pm 1.25</math> <math>9.02 \pm 0.61</math> <math>0.22 \pm 0.75</math> <math>2.9 \pm 0.07</math></th> <th>M-SimBA attack data (human eye imperceivable perturbations) FCD encrypted data Fig 3. V</th> <th>Stop (90.7%).</th> <th>Overtaking K (89.4%)</th> <th>Bicycle crossing (92.9%) IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII</th> <th>Speed limit 100 (91.6%) IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII</th> <th>beer crossing (89.8%)</th>	<b>59</b> ±1.96	erent FCD (ours) $0.85 \pm 0.99$ $1.27 \pm 1.59$ $4.41 \pm 1.72$ $5.2 \pm 1.25$ $9.02 \pm 0.61$ $0.22 \pm 0.75$ $2.9 \pm 0.07$	M-SimBA attack data (human eye imperceivable perturbations) FCD encrypted data Fig 3. V	Stop (90.7%).	Overtaking K (89.4%)	Bicycle crossing (92.9%) IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Speed limit 100 (91.6%) IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	beer crossing (89.8%)	
Table Dataset	e 2. Comp F Setting -	$\begin{array}{c} arison\\ FL con\\ \hline A_p \rightarrow\\ n=m\\ \hline 3\\ 5\\ 10\\ 15\\ 25\\ \hline 3\\ 5\\ 10\\ \end{array}$	of evas figuration figuration figuration figuration 49.55±1.60 58.15±1.69 71.85±0.90 70.35±1.23 79.55±1.13 56.18±1.93 62.68±1.09 64.28±1.46	5 ion defe ons. NE 3 5 FAT [81] 0.99±0.57 1.17±0.56 2.47±0.62 8.84±1.88 13.03±1.51 0.34±1.57 2.41±1.81 7.74±1.27	enses in denote denote 0% <b>RS</b> [10] $0.94 \pm 0.71$ $1.09 \pm 0.29$ $1.86 \pm 0.51$ $3.77 \pm 1.12$ $8.93 \pm 1.53$ $0.31 \pm 0.11$ $3.59 \pm 1.75$ $6.79 \pm 0.29$	terms of i s an FL sy FCD (ours) $0.52\pm0.73$ $0.71\pm1.32$ $0.91\pm1.04$ $2.84\pm0.70$ $6.62\pm0.68$ $0.23\pm0.19$ $1.78\pm1.09$ $5.82\pm0.93$	<b>ND</b> 50.05 $\pm$ 1.34 58.25 $\pm$ 1.41 73.45 $\pm$ 0.41 72.65 $\pm$ 1.84 79.95 $\pm$ 1.05 56.58 $\pm$ 1.15 64.28 $\pm$ 1.81 69.28 $\pm$ 1.54	n utility ithout d 5 FAT [81] $1.35\pm1.11$ $1.43\pm1.47$ $4.64\pm0.43$ $9.95\pm1.18$ $13.47\pm0.97$ $0.86\pm0.66$ $4.39\pm1.42$ $3.76\pm1.65$	$(U) \downarrow u$ efense. I 0% RS [10] 0.43±1.90 1.83±1.50 4.3±1.85 5.94±1.87 14.48±1.62 0.15±1.05 2.38±0.58 7.29±1.52	Inder M-S Bold indic Bold indic FCD (ours) 0.27±1.12 1.01±0.87 3.12±0.84 4.13±1.38 7.92±1.39 0.10±0.77 1.41±0.26 1.81±1.43	SimBA at a best is $ND$ 53.25±1.10 64.25±1.83 79.35±1.80 75.25±1.17 81.55±0.67 59.48±1.53 64.68±0.59 73.78±1.62	$\begin{array}{c} \textbf{tack across}\\ tack $	535 diff 535	erent FCD (ours) $0.85 \pm 0.99$ $1.27 \pm 1.59$ $4.41 \pm 1.72$ $5.2 \pm 1.25$ $9.02 \pm 0.61$ $0.22 \pm 0.75$ $2.9 \pm 0.97$ $5.52 \pm 0.36$	M-SimBA attack data (human eye imperceivable perturbations) FCD encrypted data Fig 3. V NLSimF	Stop (90.7%) Stop (90.7%) Itausformation key pased key pased Itausformation Itaus	Covertaking F (89.4%) Cosial distance (91.4%) Con of Social distance (91.4%)	Bicycle crossing (92.9%) IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Speed limit 100 (91.6%) IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	beer crossing (89.8%)	
Table   Dataset	e 2. Comp I Setting -	$arison$ $FL con$ $A_p \rightarrow$ $a = m$ $3$ $5$ $10$ $15$ $25$ $3$ $5$ $10$ $15$ $10$ $15$ $10$ $15$ $10$ $15$ $10$ $15$ $10$ $15$ $10$ $15$ $10$ $15$ $10$ $15$ $10$ $15$ $10$ $15$	<b>ND</b> 49.55±1.60 58.15±1.69 71.85±0.90 70.35±1.23 79.55±1.13 56.18±1.93 62.68±1.09 64.28±1.46 73.78±1.12	Sion defended ons. NE 3 FAT [81] $0.99 \pm 0.57$ $1.17 \pm 0.56$ $2.47 \pm 0.62$ $8.84 \pm 1.88$ $13.03 \pm 1.51$ $0.34 \pm 1.51$ $0.34 \pm 1.57$ $2.41 \pm 1.81$ $7.74 \pm 1.27$ $7.68 \pm 0.95$	enses in denote denote 0% <b>RS</b> [10] $0.94\pm0.71$ $1.09\pm0.29$ $1.86\pm0.51$ $3.77\pm1.12$ $8.93\pm1.53$ $0.31\pm0.11$ $3.59\pm1.75$ $6.79\pm0.29$ $7.44\pm0.69$	terms of i s an FL sy FCD (ours) 0.52±0.73 0.71±1.32 0.91±1.04 2.84±0.70 6.62±0.68 0.23±0.19 1.78±1.09 5.82±0.93 0.96±1.53	<b>ND</b> 50.05±1.34 58.25±1.41 73.45±0.41 72.65±1.84 79.95±1.05 56.58±1.15 64.28±1.81 69.28±1.54 74.58±0.76	n utility thout defined of the second state o	$(U) \downarrow u$ efense. J 0% RS [10] 0.43±1.90 1.83±1.50 4.3±1.85 5.94±1.87 14.48±1.62 0.15±1.05 2.38±0.58 7.29±1.52 10.21±0.93	nder M-S Bold indic Bold indic FCD (ours) $0.27 \pm 1.12$ $1.01 \pm 0.87$ $3.12 \pm 0.84$ $4.13 \pm 1.38$ $7.92 \pm 1.39$ $0.10 \pm 0.77$ $1.41 \pm 0.26$ $1.81 \pm 1.43$ $6.33 \pm 0.73$	SimBA at a best in the second	$\begin{array}{c} \textbf{fack across} \\ \textbf{fack across} \\ \textbf{fack across} \\ \textbf{fesults.} \\ \hline 100\% \\ \textbf{FAT [81]} \\ \textbf{fat [81]} \\ 1.92 \pm 1.16 \\ 1.92 \pm 1.16 \\ 1.81 \pm 1.25 \\ fact for a constraint of a constraint$	5 <b>SS diff</b> <b>SS diff</b> <b>SS diff</b> <b>S [10]</b> <b>S [10]</b> <b>J</b> <b>.</b> 74±1.23 <b>.</b> 32±1.61 <b>.</b> 93±1.31 <b>.</b> 83±1.03 <b>1</b> .3±0.27 <b>.</b> 96±1.70 <b>.</b> 59±1.86 <b>.</b> 39±0.98 <b>.</b> 15±1.72	erent FCD (ours) $0.85 \pm 0.99$ $1.27 \pm 1.59$ $4.41 \pm 1.72$ $5.2 \pm 1.25$ $9.02 \pm 0.61$ $0.22 \pm 0.75$ $2.9 \pm 0.97$ $5.52 \pm 0.36$ $9.28 \pm 1.01$	M-SimBA attack data (human eye imperceivable perturbations) FCD encrypted data Fig 3. V N-SimB	Stop (90.7%) Stop (90.7%) Second Second Second Second Stop (90.7%) Second Sec	Social distance (91.4%) On of sarial	Sicycle crossing (92.9%)	Speed limit 100 (91.6%) Image: Speed Speed (91.6%) Image: Speed Speed (91.6%) Image: Speed Speed (91.6%) Image: Speed Speed (91.6%) Image: Speed Speed (91.6%) Image: Speed Sp	beer crossing (89.8%)	
Table   Dataset	e 2. Comp F Setting -	arison FL con Constant Const	<b>Of evas</b> <b>figurat</b> <b>figurat</b> <b>ND</b> 49.55±1.60 58.15±1.69 71.85±0.90 70.35±1.23 79.55±1.13 56.18±1.93 62.68±1.09 64.28±1.46 73.78±1.12 74.28±0.45	Sion defe ons. NE 3 FAT [81] $0.99 \pm 0.57$ $1.17 \pm 0.56$ $2.47 \pm 0.62$ $8.84 \pm 1.88$ $13.03 \pm 1.51$ $0.34 \pm 1.51$ $0.34 \pm 1.57$ $2.41 \pm 1.81$ $7.74 \pm 1.27$ $7.68 \pm 0.95$ $14.33 \pm 0.40$	enses in denote denote 0% <b>RS</b> [10] $0.94\pm0.71$ $1.09\pm0.29$ $1.86\pm0.51$ $3.77\pm1.12$ $8.93\pm1.53$ $0.31\pm0.11$ $3.59\pm1.75$ $6.79\pm0.29$ $7.44\pm0.69$ $17.79\pm1.73$	terms of i s an FL sy FCD (ours) $0.52\pm0.73$ $0.71\pm1.32$ $0.91\pm1.04$ $2.84\pm0.70$ $6.62\pm0.68$ $0.23\pm0.19$ $1.78\pm1.09$ $5.82\pm0.93$ $0.96\pm1.53$ $8.08\pm0.11$	<b>ND</b> $50.05\pm1.34$ $58.25\pm1.41$ $73.45\pm0.41$ $72.65\pm1.84$ $79.95\pm1.05$ $56.58\pm1.15$ $64.28\pm1.81$ $69.28\pm1.54$ $74.58\pm0.76$ $76.98\pm0.35$	n utility ithout do ithout do 5 FAT [81] $1.35\pm1.11$ $1.43\pm1.47$ $4.64\pm0.43$ $9.95\pm1.18$ $13.47\pm0.97$ $0.86\pm0.66$ $4.39\pm1.42$ $3.76\pm1.65$ $8.62\pm0.19$ $15.11\pm0.92$	$(U) \downarrow u$ efense. J 0% <b>RS [10]</b> 0.43±1.90 1.83±1.50 4.3±1.85 5.94±1.87 14.48±1.62 0.15±1.05 2.38±0.58 7.29±1.52 10.21±0.93 23.61±0.15	Inder M-S Bold indic Bold indic FCD (ours) 0.27±1.12 1.01±0.87 3.12±0.84 4.13±1.38 7.92±1.39 0.10±0.77 1.41±0.26 1.81±1.43 6.33±0.73 9.28±1.79	SimBA at a best in the second	tack acro results.1009FAT [81]II $1.92 \pm 1.16$ 1 $3.01 \pm 0.34$ 2 $7.88 \pm 1.13$ 5 $11.81 \pm 1.25$ 7 $17.12 \pm 0.94$ 1 $1.03 \pm 1.36$ 0 $3.38 \pm 1.64$ 4 $9.72 \pm 1.15$ 7 $11.92 \pm 1.57$ 13 $18.86 \pm 1.93$ 24	<b>5 S S G S S G S S G S S G S S S S S S S S S S</b>	erent FCD (ours) 0.85 $\pm$ 0.99 1.27 $\pm$ 1.59 4.41 $\pm$ 1.72 5.2 $\pm$ 1.25 9.02 $\pm$ 0.61 0.22 $\pm$ 0.75 2.9 $\pm$ 0.97 5.52 $\pm$ 0.36 9.28 $\pm$ 1.01 11.58 $\pm$ 0.17	M-SimBA attack data (human eye imperceivable perturbations) FCD encrypted data Fig 3. V M-SimE GTSRB	stop (90.7%) Stop (90.7%) Seeden was pased was pased	Overtaking F (89.4%) Social distance (91.4%) Social distance (91.4%)	Sicycle crossing (92.9%)	Speed limit 100 (91.6%) Image: Speed Speed (91.6%) Image: Speed Speed (91.6%) Image: Speed Speed (91.6%) Image: Speed Sp	rossing (89.8%)	





**Connect with me on LinkedIn:**