INTRODUCTION
As the number of IoT devices being introduced in the market has increased dramatically, inference as service (IAS) has been widely used in many sensitive environments to make decisions in the cloud [1]. In IAS, devices will send data to cloud and machine learning algorithms can be run on the cloud providers’ infrastructure where training and deploying machine learning models are performed on cloud servers. However, two important issues, namely data privacy and fairness, need to be properly addressed. Our goal is to address the fairness and privacy issues simultaneously in the IAS design based on our previous work [2]. Instead of sending data directly to the server, the user will pre-process the data through a transformation map. Then we analyze the trade-off among data utility, fairness representation and privacy protection, formulate an optimization problem, and design an iterative algorithm to find the optimal transformation map.

PROBLEM FORMULATION
Consider an inference problem, in which one would like to infer the parameter $S \in S$ of data $Y \in Y$, where $Y$ is a finite set. At the meantime, there is a sensitive attribute $Z$ which contains sensitive information such as race, gender, etc. Instead of sending $Y$ directly to the server, we will learn a transformation map from $Y$ to $U \in U$, and send $U$ to the server. The server will use $U$ to conduct the inference task and the transformation mapping serves two purposes: fair presentation and privacy protection.

The optimization problem is

$$\max_{F,U|Y} F[U|Y] = I(S; U) - \beta E_{Y,U} [f(p(y|u))] - \alpha I(Z; U), \tag{1}$$

s.t. $p(u|y) \geq \epsilon, \forall y, u, \sum_u p(u|y) = 1, \forall y \in Y$.

where $d(y, u) = f(p(y|u))$ and $f$ is a continuous function defined on $(0, +\infty)$.

PROPOSED METHODS
As the objective function in (1) is a complicated non-convex function of $P_{U|Y}$, we first transform the maximization over single argument to an alternative maximization problem over multiple arguments. Then the Alternating Direction Method of Multipliers (ADMM) method is introduced to solve the sub-problems.

The objective function in (1) can be rewritten as

$$F[P_{U|Y}, P_{U|S}, P_{S|U}, P_{S|Z}] = I(S; Y) + \beta E_{Y,U}[d(y, u)] - \sum_{y,u} p(y)p(u|y)DKL[p(y|u) \parallel p(u)] - \alpha I(Z; U).$$

For consistency, we require

$$p(u) = \sum_y p(u|y)p(y), \forall u \tag{2}$$

$$p(z|u) = \sum_y p(u|y)p(z|y, u) \tag{3}$$

$$p(s|u) = \sum_y p(u|y)p(s|y, u) \tag{4}$$

Lemma 1 Suppose that $f(\cdot)$ is a strictly convex function. Then for given $P_{U|S}, P_{U|Z}, P_{S|U}, F[P_{U|Y}, P_{U|S}, P_{S|U}, P_{S|Z}]$ is concave in each $P_{U|S}, Y, \forall y \in Y$. Similarly, for given $P_{U|Y}, P_{U|S}, P_{S|U}, F[P_{U|Y}, P_{U|S}, P_{S|U}, P_{S|Z}]$ is concave in $P_{U|S}$.

For given $P_{U|Y}, P_{U|S}, F[P_{U|Y}, P_{U|S}, P_{S|U}, P_{S|Z}]$ is concave in $P_{S|U}$.

Under this property, we convert the original maximization problem to

$$\max_{P_{U|Y}, P_{U|S}} \max_{P_{S|U}, P_{S|Z}} F[P_{U|Y}, P_{U|S}, P_{S|U}, P_{S|Z}]$$

s.t. $p(u|y) \geq \epsilon, \forall y, u, \sum_u p(u|y) = 1, \forall y,$

$p(u) > 0, \forall u, \sum_u p(u) = 1$. \tag{2}$

In the second step, we obtain $p^{(i+1)}_{S|U}$ by the consistency equation (3).

In the third step, obtain $p^{(i+1)}_{S|I}$ by solving

$$\max_{P_{S|U}} F[p^{(i+1)}_{S|U}], \tag{6}$$

s.t. $p(s|u) \geq \epsilon, \forall u, s, \sum_s p(s|u) = 1, \forall u$. \tag{4}$

which has a closed form solution that is the same as the consistency equation (4).

ACKNOWLEDGEMENT
This work was supported in part by National Science Foundation under Grants CCF-1717943, CNS-1824553, CCF-1908258 and ECCS-2000415. Email: yulujin,lalai@ucdavis.edu.

REFERENCE

CONCLUSION
We have explored the utility, fairness and privacy trade-off in IAS scenarios under sensitive environments. We have formulated an optimization problem to find the desirable transformation map. We have transformed the formulated non-convex optimization problem and designed an iterative method to solve it. Moreover, we have provided numerical results showing that the proposed method can mitigate the bias and has better performance than GA in the convergence speed, solution quality and algorithm stability.