COMP 3632 – Principles of Cybersecurity

Ali Symeri

20591029

Written assignment

1.

(a)

Since you don't want to reveal your personal eating habits to the company, it means that your data (D) is sensitive. For that case, k-anonymity and differential privacy may be relevant to use by the new company to protect you. K-anonymity will ensure that distorted data is published to the company that wants to use your information and so it makes it hard to know it is your information. Differential privacy will ensure that not every query to your data is acceptable and there will be noise added to the output.

(b)

Here you want to know the others information but not reveal your own and you are able to cooperate to get the results. So, for this, Secure multiparty computation will be the best fit. As there are two parties that want to know about each other while keeping their own information secret and are willing to cooperate.

(c)

In this case, it is problematic if DNS server buys the domain that you want if you query for its availability. So, you would then use Privat information retrieval (PIR). It will retrieve the information regarding the availability of the domain without revealing to the DNS server your query.

(d)

Here you are working with people's personal information and cannot release it however you want. So, the best solution would be to use K-anonymity or Differential privacy. K-anonymity will help you publish their data by outputting distorted data to strengthen the anonymity of the users. Differential privacy will help to add some noise to the data so that it will be hard to know what it is, to provide more anonymity.

2.

(a)

Data = D files of same size
P = percentage of files changed
Sunday = full backup = D
Monday = differential backup = D * P
Tuesday = incremental backup = D * P
Wednesday = differential backup = 3 * D * P
Thursday = incremental backup = D * P
Friday = differential backup = 5 * D * P
Saturday = incremental backup = D * P

(b)

I believe that the differential backups on Wednesday and Friday may be prone to having their mean changed. This is because when the size of the file changes, it will affect the differential backups as they backup based on the current time and the last full backup.

(c)

Backups on the incremental backup days, e.g. Tuesday and Thursday cannot be corrupted if we want to be able to restore data. This is because they are dependent on the last backup.

3

(a)

($8000 + ((10 * 60) * $0.002)) / 6 bitcoins = $1333.5 per bitcoin

(b)

1 048 576 bytes / 166 bytes = 6316.7 transactions in 10 minutes
6316.7 / (10 * 60) = 10.5 transactions per second => 10 transactions per second

(c)

The transactions would be the assumption from (b), transactions in 10 minutes, 6316.7
We assume $1333.5 per bitcoin from (a) and get the price for the halved reward, so $1333.5 / 2 = $666.8 per bitcoin
So, the mean transaction fee would be $1333.5 / 6316.7 = $0.2 per transaction

(d)

No idea