Chap3#1: Privacy Preservation in Machine Learning #1

February 4, 2023

Devesh C Jinwala,
Professor, SVNIT and Adjunct Prof., CSE, IIT Jammu

Department of Computer Science and Engineering,
Sardar Vallabhhai National Institute of Technology, SURAT

Chap 2: ML Applications in Security: Topics to study

- Privacy Preservation, What is Privacy? Data Privacy. Machine Learning in Privacy Preservation: Four Main stakes to Privacy preservation in ML. Two principle approaches: (a) Augmenting the ML techniques with the conventional approaches in the domain of privacy preservation to achieve privacy viz. Homomorphic Encryption, Secret Multiparty Computations, Zero Knowledge Proofs, Perturbation techniques (e.g. differential privacy) Anonymization techniques (e.g.)k-Anonymity, l-Diversity) (b) ML-specific approaches like Federated Learning OR Ensemble Learning. Homomorphic Encryption Algorithms and the associated mathematics. Ethical issues and Law for data / process privacy : GDPR, Alexa, other relevant applications [6 hours]

ML Paradigms for Privacy Preservation

What is privacy ?

Privacy

- is the control over the extent, timing, and circumstances of sharing oneself (physically, behaviourally, or intellectually) with others.

What is privacy ?

Privacy

- is the control over the extent, timing, and circumstances of sharing oneself (physically, behaviourally, or intellectually) with others.
- Examples of activities considered private might include

What is privacy ?

Privacy

- is the control over the extent, timing, and circumstances of sharing oneself (physically, behaviourally, or intellectually) with others.
- Examples of activities considered private might include
  - a medical examination;

What is privacy ?

Privacy

- is the control over the extent, timing, and circumstances of sharing oneself (physically, behaviourally, or intellectually) with others.
- Examples of activities considered private might include
  - a medical examination;
  - activities within your home;

What is privacy ?

Privacy

- is the control over the extent, timing, and circumstances of sharing oneself (physically, behaviourally, or intellectually) with others.
- Examples of activities considered private might include
  - a medical examination;
  - activities within your home;
  - using a restaurant bathroom;

What is privacy ?

Privacy

- is the control over the extent, timing, and circumstances of sharing oneself (physically, behaviourally, or intellectually) with others.
- Examples of activities considered private might include
  - a medical examination;
  - activities within your home;
  - using a restaurant bathroom;
  - entering the office of a reproductive health provider;

What is privacy ?

Privacy

- is the control over the extent, timing, and circumstances of sharing oneself (physically, behaviourally, or intellectually) with others.
- Examples of activities considered private might include
  - a medical examination;
  - activities within your home;
  - using a restaurant bathroom;
  - entering the office of a reproductive health provider;
  - generally any action for which you have the reasonable expectation of privacy.

What is privacy ?

Privacy

- is the control over the extent, timing, and circumstances of sharing oneself (physically, behaviourally, or intellectually) with others.
- Examples of activities considered private might include
  - a medical examination;
  - activities within your home;
  - using a restaurant bathroom;
  - entering the office of a reproductive health provider;
  - generally any action for which you have the reasonable expectation of privacy.
- Data Privacy. What are the examples of data privacy ?

What is privacy ?

Privacy

- is the control over the extent, timing, and circumstances of sharing oneself (physically, behaviourally, or intellectually) with others.
- Examples of activities considered private might include
  - a medical examination;
  - activities within your home;
  - using a restaurant bathroom;
  - entering the office of a reproductive health provider;
  - generally any action for which you have the reasonable expectation of privacy.
- Data Privacy. What are the examples of data privacy ?

What is privacy ?

Privacy

- is the control over the extent, timing, and circumstances of sharing oneself (physically, behaviourally, or intellectually) with others.
- Examples of activities considered private might include
  - a medical examination;
  - activities within your home;
  - using a restaurant bathroom;
  - entering the office of a reproductive health provider;
  - generally any action for which you have the reasonable expectation of privacy.
- Data Privacy. What are the examples of data privacy ?

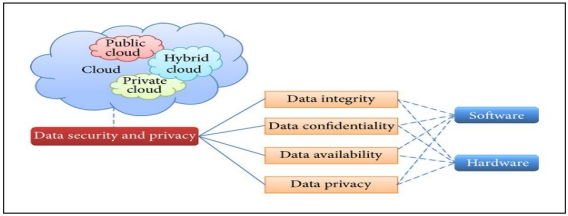


Figure: Data Security Attributes and Privacy

Data Privacy & Data Security

Data Privacy

- applies to the personal information of an individual e.g.

Data Privacy & Data Security

Data Privacy

- applies to the personal information of an individual e.g.
  - an individual's full name, mailing address, browsing history, health information, political affiliation, biometric data, and sexual orientation etc.

Data Privacy & Data Security

Data Privacy

- applies to the personal information of an individual e.g.
  - an individual's full name, mailing address, browsing history, health information, political affiliation, biometric data, and sexual orientation etc.
- comes into play when one asks from others (or collects via cookies or from third parties)

Data Privacy & Data Security

Data Privacy

- applies to the personal information of an individual e.g.
  - an individual's full name, mailing address, browsing history, health information, political affiliation, biometric data, and sexual orientation etc.
- comes into play when one asks from others (or collects via cookies or from third parties)
  - what kind of information,

Data Privacy & Data Security

Data Privacy

- applies to the personal information of an individual e.g.
  - an individual's full name, mailing address, browsing history, health information, political affiliation, biometric data, and sexual orientation etc.
- comes into play when one asks from others (or collects via cookies or from third parties)
  - what kind of information,
  - why ask for that information in the first place, and

Data Privacy & Data Security

Data Privacy

- applies to the personal information of an individual e.g.
  - an individual's full name, mailing address, browsing history, health information, political affiliation, biometric data, and sexual orientation etc.
- comes into play when one asks from others (or collects via cookies or from third parties)
  - what kind of information,
  - why ask for that information in the first place, and
  - how to plan to use the information gathered

Data Privacy & Data Security

Data Privacy

- applies to the personal information of an individual e.g.
  - an individual's full name, mailing address, browsing history, health information, political affiliation, biometric data, and sexual orientation etc.
- comes into play when one asks from others (or collects via cookies or from third parties)
  - what kind of information,
  - why ask for that information in the first place, and
  - how to plan to use the information gathered
  - how to ensure the information collected is used for the purpose intended.

Data Privacy & Data Security

Data Privacy

- applies to the personal information of an individual e.g.
  - an individual's full name, mailing address, browsing history, health information, political affiliation, biometric data, and sexual orientation etc.
- comes into play when one asks from others (or collects via cookies or from third parties)
  - what kind of information,
  - why ask for that information in the first place, and
  - how to plan to use the information gathered
  - how to ensure the information collected is used for the purpose intended.

Data Privacy & Data Security

Data Privacy

- applies to the personal information of an individual e.g.
  - an individual's full name, mailing address, browsing history, health information, political affiliation, biometric data, and sexual orientation etc.
- comes into play when one asks from others (or collects via cookies or from third parties)
  - what kind of information,
  - why ask for that information in the first place, and
  - how to plan to use the information gathered
  - how to ensure the information collected is used for the purpose intended.

Data security, on the other hand

- concerns how a company protects the data from unauthorized access or corruption.

Data Privacy & Data Security

Data Privacy

- applies to the personal information of an individual e.g.
  - an individual's full name, mailing address, browsing history, health information, political affiliation, biometric data, and sexual orientation etc.
- comes into play when one asks from others (or collects via cookies or from third parties)
  - what kind of information,
  - why ask for that information in the first place, and
  - how to plan to use the information gathered
  - how to ensure the information collected is used for the purpose intended.

Data security, on the other hand

- concerns how a company protects the data from unauthorized access or corruption.
- what one does with the data gathered from others

Data Privacy & Data Security

Data Privacy

- applies to the personal information of an individual e.g.
  - an individual's full name, mailing address, browsing history, health information, political affiliation, biometric data, and sexual orientation etc.
- comes into play when one asks from others (or collects via cookies or from third parties)
  - what kind of information,
  - why ask for that information in the first place, and
  - how to plan to use the information gathered
  - how to ensure the information collected is used for the purpose intended.

Data security, on the other hand

- concerns how a company protects the data from unauthorized access or corruption.
- what one does with the data gathered from others
  - where one stores the data, whether or not it is encrypted, who has access to it, and how one determines who is an authorized user.

Data Privacy & Data Security...

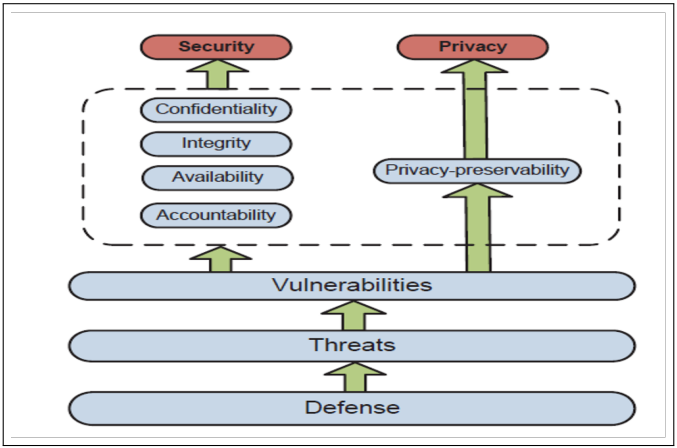


Figure: Data Security Attributes and Privacy [1]

[1] Ref: Z. Xiao et al, IEEE CS & T, April 2012

Data Privacy means ?

Multiple privacy goals

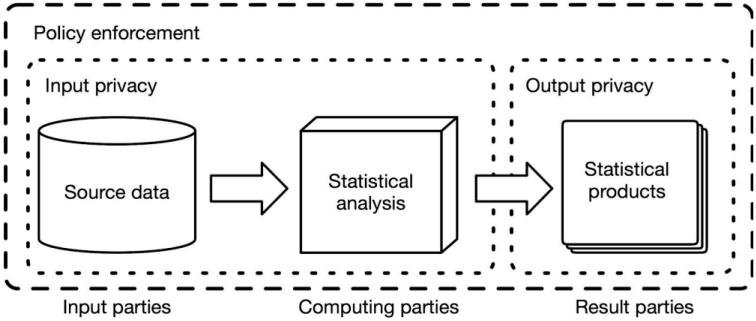


Figure 4: How multiple privacy goals co-exist in a system

Figure: How multiple privacy goals co-exist in a system? [1]

[1] Src: BigData UN Global Working Group Report

Privacy Preserving Machine Learning: Motivation

Privacy-Preserving Machine Learning

- With the benefits of machine learning applications always there is a risk of loss of data privacy

Privacy Preserving Machine Learning: Motivation

Privacy-Preserving Machine Learning

- With the benefits of machine learning applications always there is a risk of loss of data privacy
- performance of an ML algorithm vis-a-vis quality & quantity of data used for training ML models vis-a-vis need for procuring such data from different organizations

Privacy Preserving Machine Learning: Motivation

Privacy-Preserving Machine Learning

- With the benefits of machine learning applications always there is a risk of loss of data privacy
- performance of an ML algorithm vis-a-vis quality & quantity of data used for training ML models vis-a-vis need for procuring such data from different organizations
- hence, preserving privacy of data is nontrivial

Privacy Preserving Machine Learning: Motivation

Privacy-Preserving Machine Learning

- With the benefits of machine learning applications always there is a risk of loss of data privacy
- performance of an ML algorithm vis-a-vis quality & quantity of data used for training ML models vis-a-vis need for procuring such data from different organizations
- hence, preserving privacy of data is nontrivial
- an example.....

Privacy Preserving Machine Learning: Motivation

Privacy-Preserving Machine Learning

- With the benefits of machine learning applications always there is a risk of loss of data privacy
- performance of an ML algorithm vis-a-vis quality & quantity of data used for training ML models vis-a-vis need for procuring such data from different organizations
- hence, preserving privacy of data is nontrivial
- an example.....
  - Governor of Massachusetts was identified using apparently anonymized health data records containing only his birth date, gender, and ZIP code in a study done by Latanya Sweeney.....

Source: "Law, Ethics & Science of Re-identification Demonstrations". Bill of Health: Examining the Intersection of Health Law, Biotechnology and Bioethics, Petrie Flom Center at Harvard University. Retrieved 2021-06-12.

Privacy Preserving Machine Learning: Motivation...

Threats due to data sets in Privacy-Preserving Machine Learning due to

- probability of large sets of data - used for training - becoming available publicly

Privacy Preserving Machine Learning: Motivation...

Threats due to data sets in Privacy-Preserving Machine Learning due to

- probability of large sets of data - used for training - becoming available publicly
- criticality of privacy in domains like healthcare or intrusion detection systems

Privacy Preserving Machine Learning: Motivation...

Threats due to data sets in Privacy-Preserving Machine Learning due to

- probability of large sets of data - used for training - becoming available publicly
- criticality of privacy in domains like healthcare or intrusion detection systems
- probability of profit making by identifying InRedpeople or other valuable information based on the stolen data

Privacy Preserving Machine Learning: Motivation...

Threats due to data sets in Privacy-Preserving Machine Learning due to

- probability of large sets of data - used for training - becoming available publicly
- criticality of privacy in domains like healthcare or intrusion detection systems
- probability of profit making by identifying InRedpeople or other valuable information based on the stolen data
  - e.g. for medical image classification, the model must be trained using thousands, millions or even billions of example images - that if exposed to insurance providers - can lead to malicious gains.

Privacy Preserving Machine Learning: Motivation...

Threats due to data sets in Privacy-Preserving Machine Learning due to

- probability of large sets of data - used for training - becoming available publicly
- criticality of privacy in domains like healthcare or intrusion detection systems
- probability of profit making by identifying InRedpeople or other valuable information based on the stolen data
  - e.g. for medical image classification, the model must be trained using thousands, millions or even billions of example images - that if exposed to insurance providers - can lead to malicious gains.
- in addition, the ML models themselves pose a vulnerability since sensitive data may be extracted from them

Privacy Preserving Machine Learning: Motivation...

Threats due to data sets in Privacy-Preserving Machine Learning due to

- probability of large sets of data - used for training - becoming available publicly
- criticality of privacy in domains like healthcare or intrusion detection systems
- probability of profit making by identifying InRedpeople or other valuable information based on the stolen data
  - e.g. for medical image classification, the model must be trained using thousands, millions or even billions of example images - that if exposed to insurance providers - can lead to malicious gains.
- in addition, the ML models themselves pose a vulnerability since sensitive data may be extracted from them

Privacy Preserving Machine Learning: Motivation...

Threats due to data sets in Privacy-Preserving Machine Learning due to

- probability of large sets of data - used for training - becoming available publicly
- criticality of privacy in domains like healthcare or intrusion detection systems
- probability of profit making by identifying InRedpeople or other valuable information based on the stolen data
  - e.g. for medical image classification, the model must be trained using thousands, millions or even billions of example images - that if exposed to insurance providers - can lead to malicious gains.
- in addition, the ML models themselves pose a vulnerability since sensitive data may be extracted from them

Hence, the ML algorithms used, must be privacy preserving.

Four Main stakes to Privacy preservation

There are four main stakes to privacy preservation in general:

- Privacy of the input data, input queries , web search queries
- Privacy of the computations
- Privacy of the output data, web search query results
- Data Privacy General Regulations, Data protection strategies, processes and principles

Four Main stakes to Privacy preservation

There are four main stakes to privacy preservation in general:

- Privacy of the input data, input queries , web search queries
- Privacy of the computations
- Privacy of the output data, web search query results
- Data Privacy General Regulations, Data protection strategies, processes and principles

We examine one of these viz. Privacy of Computations in greater detail shortly hereafter seeing main stakes to Privacy preservation in ML

Four Main stakes to Privacy preservation in ML

There are four main stakes to privacy preservation in general:

- Privacy of the input data
  - the assurance that other parties, including the model developer, will not be able to see a user's input data
- Privacy of the output data
  - the assurance that the output of a model is only accessible to the client whose data is being inferred upon.
- Privacy of the model
  - rhe assurance that a hostile party will not be able to steal the model
- Data privacy in training
  - the assurance that a malicious party will not reverse-engineer the training data - although gathering information about training data and model is more difficult than that for the data.

But, before attempting to understand each of these let us pause for a moment and try to understand the taxonomy of approaches to privacy preservation in ML

Machine Learning & Privacy Preservation

Machine Learning & Privacy Preservation

Must be studied in terms of two closely related aspects viz.

- Augmenting the ML techniques with the conventional approaches in the domain of privacy preservation to achieve privacy

Machine Learning & Privacy Preservation

Must be studied in terms of two closely related aspects viz.

- Augmenting the ML techniques with the conventional approaches in the domain of privacy preservation to achieve privacy
- Using ML techniques that are preserving privacy e.g.

Machine Learning & Privacy Preservation

Must be studied in terms of two closely related aspects viz.

- Augmenting the ML techniques with the conventional approaches in the domain of privacy preservation to achieve privacy
- Using ML techniques that are preserving privacy e.g.
  - Federated learning OR Ensemble techniques - that inherently help realize privacy preservation

Machine Learning & Privacy Preservation

Must be studied in terms of two closely related aspects viz.

- Augmenting the ML techniques with the conventional approaches in the domain of privacy preservation to achieve privacy
- Using ML techniques that are preserving privacy e.g.
  - Federated learning OR Ensemble techniques - that inherently help realize privacy preservation
  - but the ones that also ensure machine learning training that keeps user data private.

Privacy-Preserving Machine Learning

- is a step-by-step approach to preventing data leakage in ML algorithms.

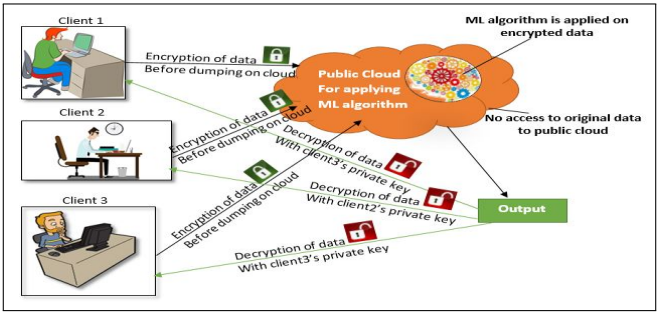


Figure: Privacy Preserving ML

Src: https://www.analyticsvidhya.com/blog/2022/02/privacy-preserving-in-machine-learning-ppml/

Privacy-Preserving Machine Learning

- is a step-by-step approach to preventing data leakage in ML algorithms.
- allows many privacy-enhancing strategies to allow multiple input sources to train ML models cooperatively without exposing their private data in its original form.

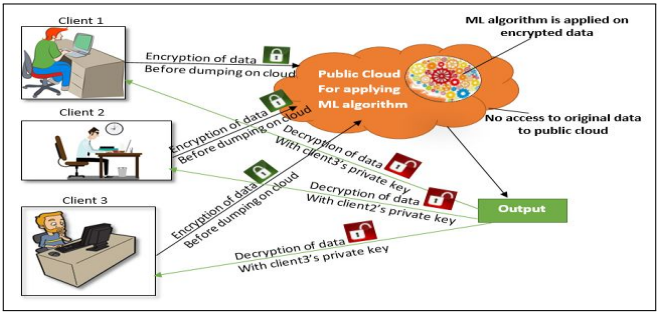


Figure: Privacy Preserving ML

Src: https://www.analyticsvidhya.com/blog/2022/02/privacy-preserving-in-machine-learning-ppml/

Privacy Preserving Machine Learning: How to achieve?

The goal of privacy-preserving machine learning is

- to bridge the gap between privacy while receiving the benefits of machine learning.

Privacy Preserving Machine Learning: How to achieve?

The goal of privacy-preserving machine learning is

- to bridge the gap between privacy while receiving the benefits of machine learning.
- is a critical facilitator for the protection of acquired data and adhering to data privacy laws.

Privacy Preserving Machine Learning: How to achieve?

The goal of privacy-preserving machine learning is

- to bridge the gap between privacy while receiving the benefits of machine learning.
- is a critical facilitator for the protection of acquired data and adhering to data privacy laws.

Privacy Preserving Machine Learning: How to achieve?

The goal of privacy-preserving machine learning is

- to bridge the gap between privacy while receiving the benefits of machine learning.
- is a critical facilitator for the protection of acquired data and adhering to data privacy laws.

Privacy-preservation in ML

- is achieved by augmenting conventional ML with different strategies that protect data privacy, that include....

Privacy Preserving Machine Learning: How to achieve?

The goal of privacy-preserving machine learning is

- to bridge the gap between privacy while receiving the benefits of machine learning.
- is a critical facilitator for the protection of acquired data and adhering to data privacy laws.

Privacy-preservation in ML

- is achieved by augmenting conventional ML with different strategies that protect data privacy, that include....
  - cryptographic approaches like

Privacy Preserving Machine Learning: How to achieve?

The goal of privacy-preserving machine learning is

- to bridge the gap between privacy while receiving the benefits of machine learning.
- is a critical facilitator for the protection of acquired data and adhering to data privacy laws.

Privacy-preservation in ML

- is achieved by augmenting conventional ML with different strategies that protect data privacy, that include....
  - cryptographic approaches like
    - homomorphic encryption

Privacy Preserving Machine Learning: How to achieve?

The goal of privacy-preserving machine learning is

- to bridge the gap between privacy while receiving the benefits of machine learning.
- is a critical facilitator for the protection of acquired data and adhering to data privacy laws.

Privacy-preservation in ML

- is achieved by augmenting conventional ML with different strategies that protect data privacy, that include....
  - cryptographic approaches like
    - homomorphic encryption
    - secure multi-party computing,

Privacy Preserving Machine Learning: How to achieve?

The goal of privacy-preserving machine learning is

- to bridge the gap between privacy while receiving the benefits of machine learning.
- is a critical facilitator for the protection of acquired data and adhering to data privacy laws.

Privacy-preservation in ML

- is achieved by augmenting conventional ML with different strategies that protect data privacy, that include....
  - cryptographic approaches like
    - homomorphic encryption
    - secure multi-party computing,
    - Zero knowledge proofs

Privacy Preserving Machine Learning: How to achieve?

The goal of privacy-preserving machine learning is

- to bridge the gap between privacy while receiving the benefits of machine learning.
- is a critical facilitator for the protection of acquired data and adhering to data privacy laws.

Privacy-preservation in ML

- is achieved by augmenting conventional ML with different strategies that protect data privacy, that include....
  - cryptographic approaches like
    - homomorphic encryption
    - secure multi-party computing,
    - Zero knowledge proofs
  - perturbation techniques like differential privacy

Privacy Preserving Machine Learning: How to achieve?

The goal of privacy-preserving machine learning is

- to bridge the gap between privacy while receiving the benefits of machine learning.
- is a critical facilitator for the protection of acquired data and adhering to data privacy laws.

Privacy-preservation in ML

- is achieved by augmenting conventional ML with different strategies that protect data privacy, that include....
  - cryptographic approaches like
    - homomorphic encryption
    - secure multi-party computing,
    - Zero knowledge proofs
  - perturbation techniques like differential privacy
  - anonymization techniques like k-Anonymity and l-Diversity

Privacy Preserving Machine Learning: How to achieve?

The goal of privacy-preserving machine learning is

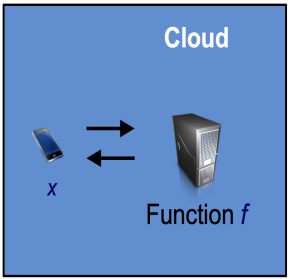
- to bridge the gap between privacy while receiving the benefits of machine learning.
- is a critical facilitator for the protection of acquired data and adhering to data privacy laws.

Privacy-preservation in ML

- is achieved by augmenting conventional ML with different strategies that protect data privacy, that include....
  - cryptographic approaches like
    - homomorphic encryption
    - secure multi-party computing,
    - Zero knowledge proofs
  - perturbation techniques like differential privacy
  - anonymization techniques like k-Anonymity and l-Diversity
  - ML-specific approaches like Federated Learning OR Ensemble Learning - the Privacy-Preserving Techniques - modifying the conventional ML training methods to keep user data private.

Augmenting ML for Privacy Preservation: Homomorphic Encryption

Issues in outsourcing computations



- Privacy
  - Cloud should not learn anything about x

- Verifiability
  - Cloud cannot cheat i.e., return an incorrect answer without being detected

Figure: Outsourcing Computations [1]

[1] Src: Vinod Vaikunthnathan

Why privacy of computations:1 ?

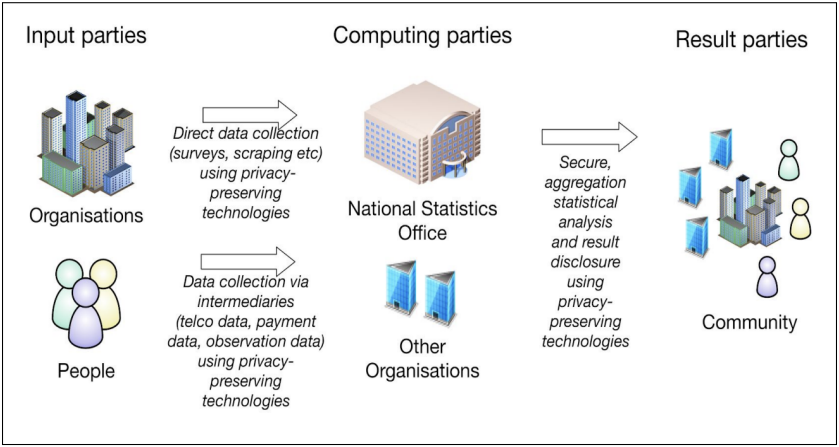


Figure: Privacy-preserving statistics workflow for a single Statistics Office [1]

[1] Src: BigData UN Global Working Group Report

Why privacy of computations:2 ?

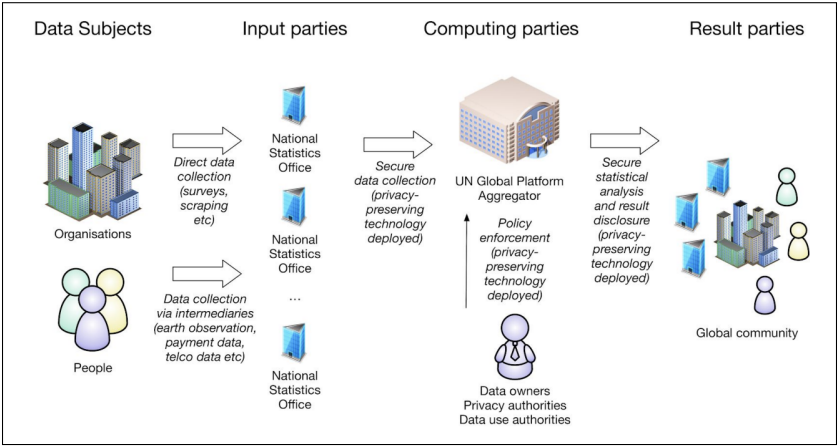


Figure: Privacy-preserving statistics workflow for a single Statistics Office [1]

[1] Src: BigData UN Global Working Group Report

Approaches to Privacy of Computations

Approaches to achieve privacy of data computations in cloud

- Cryptographic Approaches

Approaches to Privacy of Computations

Approaches to achieve privacy of data computations in cloud

- Cryptographic Approaches
  - (Fully) Homomorphic Encryption (abbreviated as HE or FHE)

Approaches to Privacy of Computations

Approaches to achieve privacy of data computations in cloud

- Cryptographic Approaches
  - (Fully) Homomorphic Encryption (abbreviated as HE or FHE)
  - Secure Multiparty Computation (abbreviated MPC)

Approaches to Privacy of Computations

Approaches to achieve privacy of data computations in cloud

- Cryptographic Approaches
  - (Fully) Homomorphic Encryption (abbreviated as HE or FHE)
  - Secure Multiparty Computation (abbreviated MPC)
  - Trusted Execution Environments (abbreviated as TEE)

Approaches to Privacy of Computations

Approaches to achieve privacy of data computations in cloud

- Cryptographic Approaches
  - (Fully) Homomorphic Encryption (abbreviated as HE or FHE)
  - Secure Multiparty Computation (abbreviated MPC)
  - Trusted Execution Environments (abbreviated as TEE)
  - Zero Knowledge Proofs (abbreviated as ZK Proofs)

Approaches to Privacy of Computations

Approaches to achieve privacy of data computations in cloud

- Cryptographic Approaches
  - (Fully) Homomorphic Encryption (abbreviated as HE or FHE)
  - Secure Multiparty Computation (abbreviated MPC)
  - Trusted Execution Environments (abbreviated as TEE)
  - Zero Knowledge Proofs (abbreviated as ZK Proofs)
- Non-cryptographic Approaches

Approaches to Privacy of Computations

Approaches to achieve privacy of data computations in cloud

- Cryptographic Approaches
  - (Fully) Homomorphic Encryption (abbreviated as HE or FHE)
  - Secure Multiparty Computation (abbreviated MPC)
  - Trusted Execution Environments (abbreviated as TEE)
  - Zero Knowledge Proofs (abbreviated as ZK Proofs)
- Non-cryptographic Approaches
  - perturbation techniques like differential privacy

Approaches to Privacy of Computations

Approaches to achieve privacy of data computations in cloud

- Cryptographic Approaches
  - (Fully) Homomorphic Encryption (abbreviated as HE or FHE)
  - Secure Multiparty Computation (abbreviated MPC)
  - Trusted Execution Environments (abbreviated as TEE)
  - Zero Knowledge Proofs (abbreviated as ZK Proofs)
- Non-cryptographic Approaches
  - perturbation techniques like differential privacy
  - anonymization techniques like k-Anonymity and l-Diversity

Outsourcing computations: Requirements

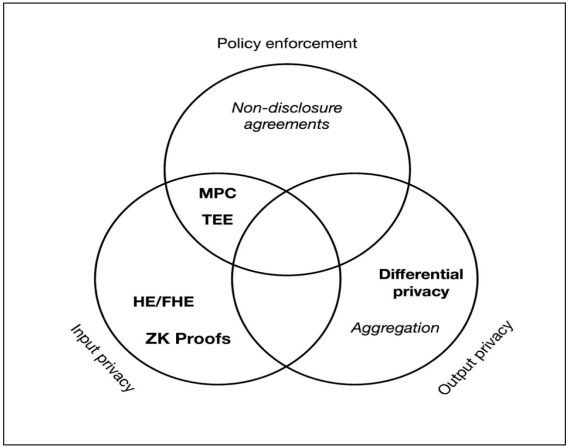
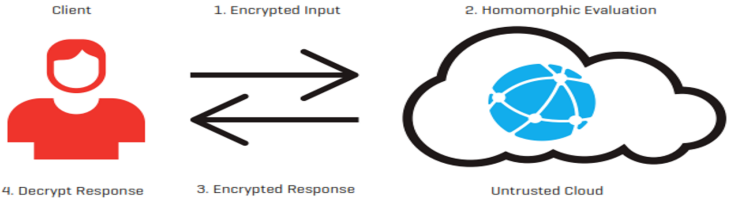


Figure: Venn diagram showing which privacy goals are fulfilled by which privacy techniques. [1]

[1] Src: BigData UN Global Working Group Report

Outsourcing computations: Requirements

Figure 1: A natural application of fully homomorphic encryption is outsourcing computation to an untrusted third party, such as the cloud.



Such a scenario might arise when a client lacks the computational resources to carry out the computation, and thus, needs to delegate the computation to a potentially untrustworthy party. In the simplest example of outsourcing computation using the fully homomorphic encryption scheme (FHE), the client first encrypts the input using the FHE scheme, then sends the ciphertexts to the cloud, which performs the computation homomorphically. Finally, the client receives the encrypted response and decrypts it to learn the result of the computation.

Figure: Outsourcing Computations [1]

[1] CACM

Outsourcing computations: Using Homomorphic Encryption

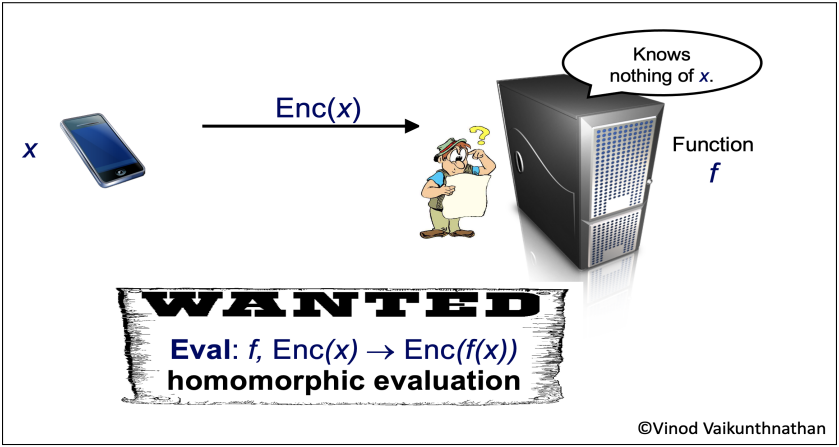


Figure: Outsourcing Computations [1]

[1] Src: Vinod Vaikunthnathan

Outsourcing computations Privately

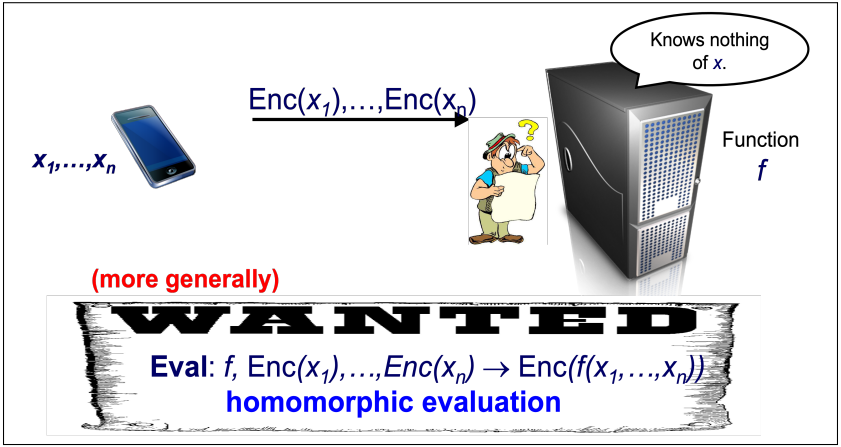


Figure: Outsourcing Computations Privately

Outsourcing computations Privately

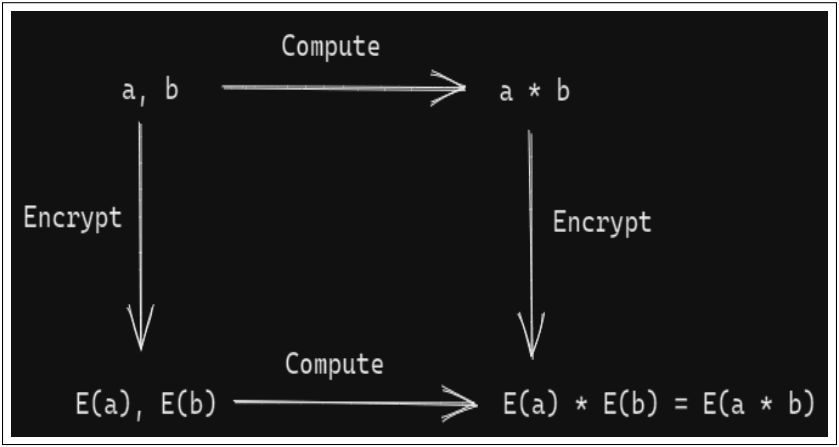


Figure: Outsourcing Computations Privately [1]

[1] Src: Vinod Vaikunthnathan

Outsourcing computations: Is Privacy Preserved?

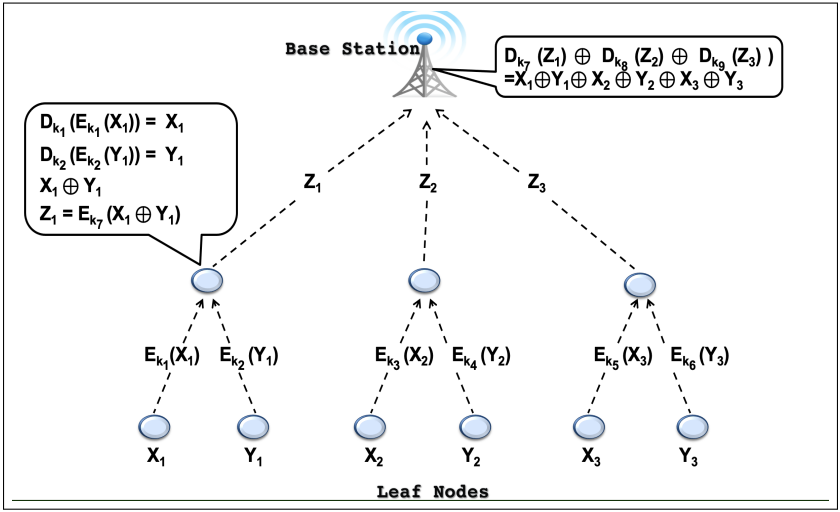


Figure: Coventional Encryption: Is Privacy preserved ?

Outsourcing computations : Is Privacy Preserved?

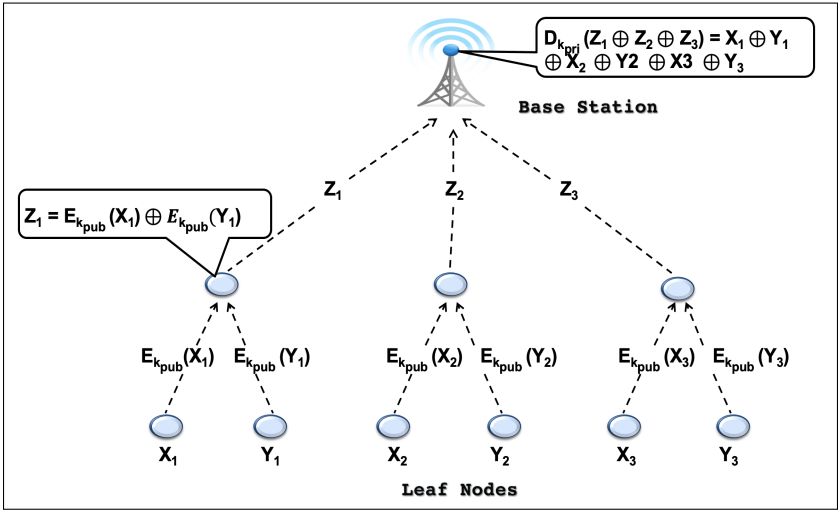


Figure: Outsourcing Computations Privately

Homomorphic Encryption Algorithms

Blank

Blank