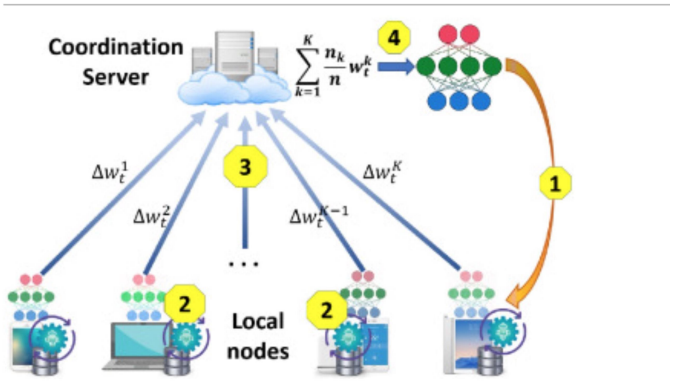
UC SCENARIO/RATIONALE

Federated Machine Learning Challenges in IoT

If everything is connected, everything can be hacked

In a general Machine Learning setup, we usually train our data that is aggregated from several edge devices and is gathered in a central server. Machine Learning algorithms then operate on this data and train itself and finally predicts results for new data generated.
On the other side, there is the Federated learning approach technique that trains an algorithm across multiple decentralized edge devices or servers holding local data samples without exchanging them. This approach stands in contrast to traditional techniques illustrated above, where all the local datasets are uploaded to one server.
Generally speaking, in Federated Machine Learning, we have a common setup which consists of a central server S and several dispersed nodes user(i), i 1, 2, … N. In this setting, the nodes exchange locally trained model updates with the central server, which undertakes the aggregation of the individual model contributions. Specifically, in each iteration, the server S sends the global model to each node UI, i 1, 2, … N. Next, the model is trained based on the private local data stored on each node. The renewed model parameters are sent back to the central server S, where all the model updates from each different node are aggregated, creating a new global model. The aforementioned procedure is repeated until satisfying a termination condition, such as reaching a specified number of iterations. The nodes participating in the FL system could be smartphones, laptops, IoT devices.
Although this method is tailored to solve the sharing of private data partially, if anyway faces several challenges.



Problem to be solved
Although data exchanges in an FL system should ensure that only model updates are exchanged, in reality the exchange of information between the devices and the server may contain sensitive information that could allow profiling of the device and consequently the user. This possibility means that also in an FL system there are problems related to privacy that must be taken into account and properly managed.
Said that, describe also, using scientific literature,
a) what is the intrinsically weakness of this architecture from the privacy point of view?
b) what could be an approach that will allow lowering the probability of privacy disclosure. This could be done by proposing an architecture or a set of functionalities to build upon the typical FL

architecture.
Solution

Commento [AC1]: Aggiungere esempi di questo

UC SCENARIO

ATOMIC SWAP Privacy Preserving

It is well known that one of the fundamental capabilities of distributed ledgers is to be able to substitute a trusted party or escrow service for parties wishing to transact.
An asset can be exchanged or held according to logic that can be programmed and that the network evaluates through a smart contract.
We consider the transfer of assets across different blockchains referred to as an atomic cross-chain swap.
One possible real use case of this scenario is the one related to the so-called utility switch. Utility switch is when a customer decides to change in real time the electricity, water, gas provider. In this case it is needed a methodology that allow this exchange make the user device system a plug and play asset and make it capable to convert energy token between different utilities (Think about a smart meter). Distributed ledger can help on design such a scenario using the so-called Hash Time Locked Contracts.
(https://en.bitcoin.it/wiki/Hash_Time_Locked_Contracts)

Problem to be solved:
As sophisticated as this technology may be, at the same time this type of protocol has profound shortcomings in terms of privacy.
Illustrate what are weakest aspect related to privacy for such an atomic swap based on HTCL when for example two parties want to convert one cryptocurrency in another and make a swap. (x ETH for y BTC)

Could you image a new protocol that allow this atomic swap without compromise privacy?

Solution		

Commento [AC2]: Devo inserire un po' di esempi che guideranno lo studente.Come fare la stessa cosa

Commento [AC3]: Aggiunto nel power point

UC SCENARIO

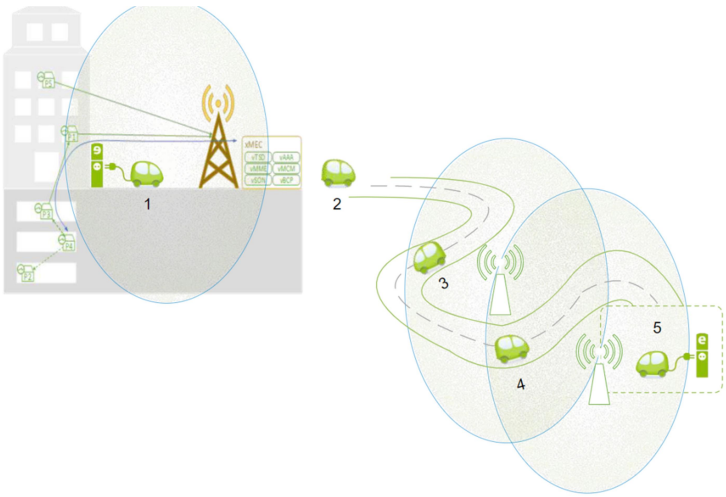
Enjoy green vehicle preserving privacy in the age of 5G

Consider a scenario where a new electric vehicle is delivered to its delighted new owner. The vehicle is dropped off at their apartment and switched on ready for its first journey. The proud owner plugs their new car into the charger and the vehicle registers itself with the local 5G base station. The owner makes sure the car is set up to register for the NRG5 energy services–it picks a service where the car keeps the NRG5 system up to date of its battery levels and the owner will receive information about suitable car charging opportunities while on the go.

Once fully charged, the new owner decides to take their family for a test drive with their shiny new green car. They are soon seen leaving the local town and heading through the remote countryside to a larger city some distance away.

In the picture below, at position (1) the new vehicle has just arrived and is charging and registering with the local base station.

At point (2) the car is on the move through a remote area where there is no 5G base station nearby, and there is no 5G access. The family is super excited. Some 75 minutes later, at position (3), the car has entered the destination city. Much to the delight of the two teenagers in the back of the car there is 5G coverage again, provided from one local base station. The car connects to the base station. Very soon, at position (4) the car finds itself within reach one further separates base station. It will now need to decide whether to change its allegiance to the newly discovered base station. Not much later, at point (5) the car is no longer within reach of the first base station of this city, and finds only coverage from one base station here. The family is getting tired, and happily the car owner receives a notification from the NRG5 energy service indicating that there is an opportunity hereto top up the battery charge, providing details of a convenient local charging point offering a special energy pricing deal at this time. The owner decides to use the facility to charge their vehicle, while using grabbing the chance to enjoy coffee and cakes with the family.



Problem to be solved

How to design a 5G platform running on the edge capable to provide the E2E service to thew car Owner? Illustrate main problems to be tackled and also how preserve privacy of the end user so to not classify or infer information related to personal behavior

UC SCENARIO

NFT TOKEN AND IoT

The term “Asset Tokenization” describes the process of replicating a real-world or financial asset in the form of a digital token. It’s possible to translate every asset, such as bonds, stocks, arts, or real estate into a digital format.
(To put it simply, tokenization converts an asset, physical or otherwise, into a token that can be manipulated within a blockchain system).
For example, a real estate developer might want to sell a property in digital form. A tokenization service provider will replicate the asset digitally by storing all of the property’s data, such as property value, building specifications, or location on a blockchain. The total asset value is then split into a specific number of tokens with each token representing a fraction of the original asset value.

The “smart contract” of the token, an encrypted and automatically enforced set of rules, will specify the rights of the token holder, for example, ownership rights or a share of rental payments.
The ERC-721 standard defines how to build NFTs on the Ethereum blockchain through a smart contract interface.
In case of an IoT device the process to create a NFT from it, is interesting because once created it bring a link between the token and device that is difficult to break and can be traced during their lifetime, because devices execute a secure boot and carry out mutual authentication processes with new owners and users that could add new software. Hence, devices prove their trusted hardware and software.

In the ERC-721 standard a tokenizable asset as an art piece can be owned and transferred and it has two main attributes: **tokenId**, which is the unique identifier of the token, and **owner,** which is the blockchain account (BCA) address that 1) owns the token, 2) can transfer ownership, and 3) can approve others (approved and operators) to act in its name.

However, when trying to represent IoT devices by NFTs the challenge sits in the fact that IoT devices cannot be considered as passive assets with unique identifiers and owners; but it need more attributes : for example, In the context of a blockchain, a main difference between an IoT device and a passive asset is that the IoT device can interact with other blockchain participants, i.e., it can have a BCA.

Problem to be solved:
Moreover the IoT devices has an active functioning I.e.(When it is activated and disactivated and produce data etc etc). Please add to the standard ERC 721 functions, attributes and events so the cover the IoT device and allow to be digitalized in the blockchain?

.

Solution	

UC SCENARIO

5G Slicing

.
5G communications not only improves the devices connection to the mobile networks but introduce the important concept of network slice. This means that mobile devices with different specification are routed through different physical and logic networks that all together are represented as a slice.

Commento [AC4]: Qui ho rifrasato il tutto l'obiettivo puo' essere duplice. Si introduce lo standard ERC721 che è uno standard di smart contract per digitalizzare asset. Quindi si definisce un semplice asset fisico tipo quadro e come viene digitalizzato seguendo lo standard ERC721. Poi introduco un IoT device che ha differenti proprietà funzioni ed eventi. SI chiede di definire come estendere ad un alto livello questo protocollo. Poi da questo si puo' ricavare un secondo esercizio . Come si puo' univocamente legare un device fisico ad una coppia chiave privata pubblica? Si puo' passare dal PUF.
Concludendo ho anche inserito delle slide che definiscono bene questo standard ERC721. Il massimo potrebbe essere far vedere uno smart contract come gira. Si puo'' usare un bel IDE online tipo https://remix.ethereum.org/
Oggi mi sento spavaldo:-)

Commento [LL5]: Mitico!

Some slices can be created for service that requires personal data: image medical data or electric vehicle sharing data about road trajectories et etc. This data should not be traced by adversaries. In one scenario like this auth schemes used in 4G are not more useful to allow people to track personal data.	
.	
Solution	