**Slide 1**

IOt: nowadays everything has id not only users but also devices , and they can interact and communicate but this communication must be secured ,

IOt devices must be uniquely identifiable to enable authenticity ,

This could be achieved through IAM.

So what is IAM : identity management in which each user has a unique digital identity that can use it in many actions and transactions , when you are trying to access resources through your identity securely this is what IAM.

* It provides 3 main components :
  + - Identity management
    - Access control
    - Monitoring and logging
* **Slide 2**

Identity Management operations. The identities of all communicating entities must be secured to prevent identity theft. Data and networks used by IoT devices must be protected by Access Control mechanisms to prevent unauthorized access to enterprise resources and confidential IoT data . Finally, IAM incorporates Monitoring

& Logging functionalities to be able to store and trace critical information in

a secure and auditable manner

**Slide 3**

Questions

**Slide 4**

1-IoT devices often do not have a high computational capacity and are low powered. Therefore, different constraints based on

their physical design arises.

2-the need for comprehensive and secure IAM mechanisms. As identities within an IoT context are very large

in number it has to be ensured that each device has a managed identity within a supervised IAM platform, information about the identity of all other devices, and the possibility to verify them. Then and only then one can provide a comprehensive view on all identities within an enterprise IoT

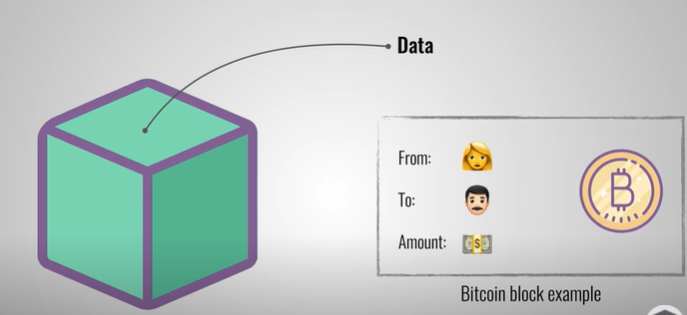
3- variability of identities.: They are highly heterogeneous as they have different attributes which need to be managed correctly.

4- scalable mechanism : An IAM platform has to ensure full operability regardless the number of managed identities and the accompanying requirements for storage and network

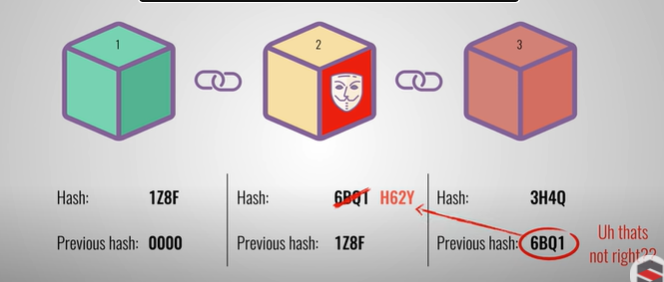
consumption.

**Slide 7**

Blockchain consists of multiple block each block contains a data ,hash and previous hash



Hash is unique changing something in the block will change the hash



Public blockchains like bitcoin where any one can access, to avoid sibyl attacks it uses POW

In a Sybil attack, the attacker subverts the reputation system of a network service by creating a large number of pseudonymous identities and uses them to gain a disproportionately large influence

POW : mechanism that slows down the creation of block , changing in one block -> recalculate all hashes of all blocks

In private blockchain networks, participants are known and whitelisted.

Node must be initially authorized by a trusted authority ,This process can be referred to as node identity management

Due to node identity management, private blockchains can rely on computationally inexpensive, voting-based consensus mechanisms, thus enabling processing of tens of thousands of transactions per second. One class of consensus mechanisms for private blockchains which is currently employed is based on the Byzantine Fault-Tolerant (BFT) Protocol

An entity which wants to submit data to the blockchain encapsulates the request into a transaction and proposes it to the validating nodes. The validating nodes enforce a given set of contract rules by the replicated execution of smart contracts.

A smart contract is a computer program or a transaction protocol which is intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement.

Identity Management :

blockchain-based identity framework for IoT (BIFIT) for smart home environments. The framework enables the management of IoT devices by their respective device owner. Owner identities are held on a blockchain and managed by transactions.

Device identities further contain the owner's signature as an attribute. This approach can be applied to all kind of IoT devices, thus ensuring interoperability.

The digital identities of owners are created by issuing a transaction to a blockchain which contains an identifier hash value, key pairs,the identity signature, and a storage pointer.

Tamper proof : you are able to see if anything has been changed opened removed or damaged

**Access Control**

Access Control. leverage blockchain to store representations of access rights to a specific resource in a tamper-proof way and to manage those rights via blockchain transactions. Access rules are employed by attribute based access control (ABAC) [14] policies. Policies consist of conditions defining a set of allowed values for attributes and specify the actions which subjects are entitled to perform on the addressed resource. Attributes can be related to the subject demanding access, the resource, or the environment. Policies are initially denied by the resource's owner who issues a policy creation transaction to the blockchain. Resource owners can update and revoke policies by issuing update or revocation transactions to the blockchain respectively. Resource owners can change their policies over time. All changes such as policy updates and right transfers are timestamped and logged to the blockchain in a traceable way. Resource owners can issue right transfer transactions which are linked to a particular subject. When receiving a subject's request for access to a resource, a policy enforcement point authenticates the subject by its id and a challenge and queries the blockchain for transactions holding relevant policy data. It then builds a standard XACML policy which is transferred to a policy decision point where it is evaluated against the subject's attributes.

leverage the blockchain technology to manage ownerships and sharings of data streams provided by IoT devices. Owners can share data streams by issuing a new transaction to the blockchain which holds the identifier of the data stream and the service's public key. The potential impact of a node acting

maliciously is limited because each node only holds a small encrypted piece of a data stream. A user who wants to revoke access rights to a data stream changes the encryption key and shares it with all authorized services except the one to be revoked. Additionally, the owner issues a new transaction which replaces

previous permissions. This also facilitates monitoring of access management activity. The blockchain does not hold these chunks but only their hash pointer to the previous chunk. It contains a hash pointer of each chunk to ensure tamperproof storage,

**Monitoring :**

Due to the decentralized nature of storage, a complete log of the issued transactions will remain in the blockchain, no matter whether a user leaves or rejoins the network over an arbitrary period of time. Access to the respective log only requires the download of the latest version of the blockchain. The blockchain log is maintained as long as there are nodes in the network

Scenario

If now, for example, a device initiates communication e.g. via smartphone of an employee to deliver sensor data, the employee can A) identify the device securely by validating its signature using the public key stored in the blockchain. B) The employee can ensure that the device was not manipulated by comparing the hash value stored in the blockchain with the hash value of the actual data delivered with the request. To protect critical resources from unauthorized access, suitable access control needs to be applied. In Figure 5, access control operations and entities are illustrated by the blue-colored arrows and entities. Our access control scheme

is based on the commonly used ABAC denied by Hu et al. [14]. The scenario starts with an administrator who creates new access control policies and issues them as transactions to the blockchain (access rules). For example, employees and devices could hold an attribute "emergency operations". A policy could then enforce that all users or devices which hold this attribute are able to access temperature sensor data of engines. However, additional attributes are necessary to read or write more critical information such as prototype blueprints

which can be sent to the construction plant.

Under the aspect of monitoring (in color red) all nodes appended to the

blockchain can be monitored as the blockchain itself can be regarded as a log

storage. Any user action gets appended to the blockchain including the identity's

unique identifier as well as additional information regarding its action. This could

be the respective entitlement that was evaluated or any further attributes avail-

able (e.g. IP address or timestamp). Malicious activities can then be detected

by comparing the identity's behavior with the historic usage pattern which re-

mains within the blockchain and can be retrieved by traversing the blockchain

and searching for all logs with the identity's unique identifier (query data for

monitoring). An advantage compared to traditional logging mechanisms is the

decentralized data storage within the blockchain. A malicious attacker cannot

easily manipulate the log collection (e.g. by deleting logs after an attack) by

targeting only one log server. Because the logs are stored on many different de-

vices via blockchain technology an attacker would need to maintain control over

a specific amount of devices (based on BFT this would be more than 33% as

discussed in Section 4.1).