CyfRA

Blockchain as a security measure for IoT systems

IoT Main Issues

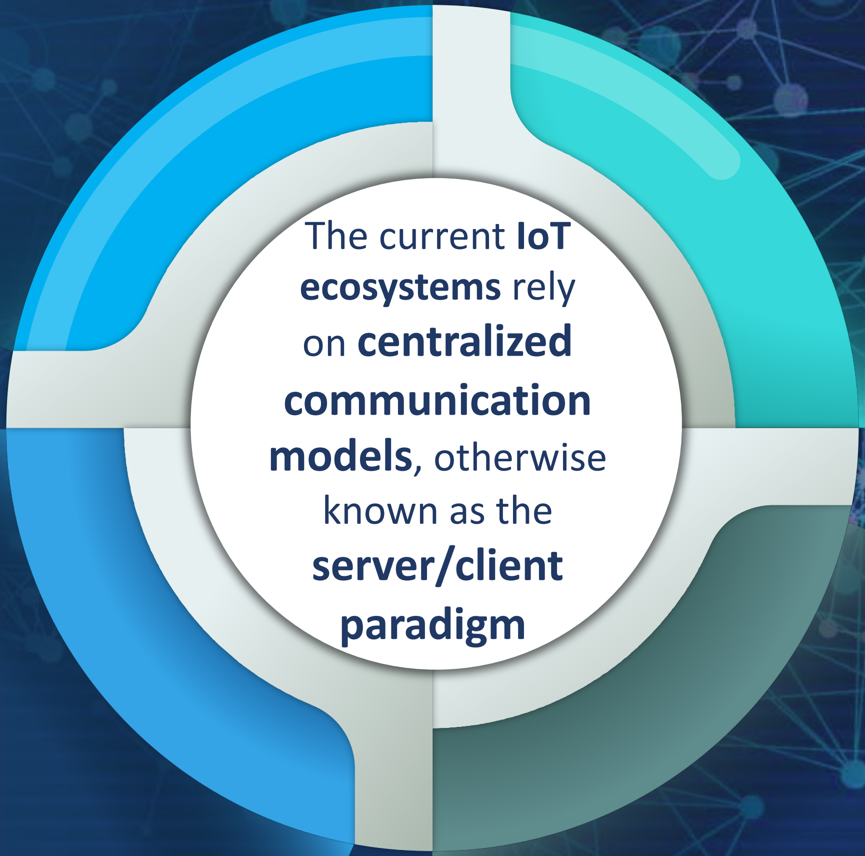
CyfRA

Security

Data flows across various kinds of devices, each having its own set of **policies** and administrative **boundaries** and stored on the cloud . In this way, it becomes complicated to ensure the safe functioning of an IoT system and the proper mgmt of data.

Privacy and Data Storage

Companies will be responsible for massive amount of consumer data left in insecure repositories. Centralized IoT ramps up the Personal Identity Information (PII) sprawl crisis that consumers fall victim to daily.



The current **IoT ecosystems** rely on **centralized communication models**, otherwise known as the **server/client paradigm**

High Costs

Existing IoT solutions are **expensive** because of the high infrastructure and maintenance cost associated with centralized **clouds**, large **server** farms and networking **equipment**

Inadequate Infrastructure

When millions objects will be Internet-connected, the number of communications will also increase, leading to issues with **scalability, economics, and engineering**

Even if these **challenges are overcome**, **cloud servers will remain a bottleneck** and there's no platform that connects all devices and no guarantee that cloud services offered by different supplier are **interoperable and compatible.**

ETSI Cyber Security for Consumer Internet of Things

Because of these possible problems, the **ETSI Cyber Security for Consumer Internet of Things** gives us some fundamental provisions, such as:

- **Provision 4.4** — To securely store credentials and sensitive data within services and on devices.
- **Provision 4.5** — To encrypt security-sensitive data in transit and to manage securely all keys and passwords
- **Provision 4.6** — To minimize exposed attack surfaces (Hardware should not unnecessarily expose access to attack; Code should be minimized to the necessary functionality for the device to operate).
- **Provision 4.8** — Ensure that personal data is protected (Device manufacturers and service providers shall provide consumers with clear and transparent information about how their personal data is being used)
- **Provision 4.11** — Make it easy for consumers to delete personal data Mechanisms can be provided to allow the consumer to remain in control and remove personal data from services
- **Provision 4.13** — Validate input data via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices

How to face IoT limits

CyfRA

How we can try to overcome this issues and respond appropriately to some of the **ETSI Cyber Security for Consumer Internet of Things provisions**?

Blockchain Technology

These problems can be faced thanks to a decentralization process and the use of

Blockchain Technology

***The Blockchain distributed ledger can*:**

- be used in **tracking** billions of **connected device** and enable the processing of transactions and coordination between devices;
- **eliminate single points of failure**, creating a more resilient ecosystem for devices to run on;
- enrich the IoT by providing a trusted sharing service, where **information is reliable and can be traceable.**
- allow data sources to be identified at any time and data **remains immutable** over time, increasing its security..

Blockchain technology is probably the **missing link to settle security, privacy and reliability concerns in the Internet of Things and could** perhaps be the **silver bullet needed by the IoT industry.**

Key benefits of Blockchain decentralization

CyfRA

Trustless

Trust between all parties and IoT devices will be built without having to place trust in a centralized service provider to store data or be in control of device connectivity.

Reduce costs

Reduce costs by removing overhead associated with intermediaries and avoid installing and maintaining large centralized data centers

Accelerate Transactions

Blockchain can accelerate the creation of an IoT ecosystem of services, where transactions settlement time is reduced from days to hear instantaneous

Reduce risk of tampering

Distributed ledger technology uses asymmetrical cryptography to timestamp and immutably store transactions.

Autonomy

Blockchains enables smart devices to act independently and self-monitor. This could remove central authority to have completely automated services.

Benefit: Focus on Improved Security

Blockchain offers the potential of greatly improving the overall security of the IoT environment thanks to:

- **highly encrypted transactions**→ considered the most secure thanks to the powerful data encryption through hashing tags, really hard to be hacked;
- **no single point of failure** → the decentralized set-up denies cyber attackers to target a single point of entry to bring down the network through spoofing and Ddos attacks;
- **cryptographic signatures** → it doesn't exist a single location, and man-in-the-middle attacks cannot be staged because there is no single thread of communication that can be intercepted;
- **node status tracking capabilities**→ to track the node status can be very useful in preempting any attempt to break into the IoT security by the malicious intruders.

Much of the **data generated by IoT is highly personal** — smart home devices have access to intimate details about our lives. This is data that needs to be shared with other devices in order to be useful to us but it also means there are far more openings for hackers potential attack.

Key challenges of Blockchain integration

CyfRA

Scalability issues

the size of Blockchain grow constantly over time and requires some kind of record management which makes necessary to come up with better designs for **scalability**.

Processing power and time

IoT ecosystems comprehend diverse devices that have very **different computing capabilities**, not all of them will be capable of running the same encryption algorithms at the desired speed.

Storage

The blockchain ledger has to be **stored** on each node of the system and it will increase in size as time passes. That is beyond the capabilities of a wide range of smart devices

Lack of skills

Few people understand how Blockchain technology really works especially with IoT. It becomes **challenging** to **hire** the **required teams** to administrate and run Blockchain projects.

Legal and compliance issues

It's a new territory **without** any **legal** or **compliance precedents** to follow. It poses a serious problem for IoT manufacturers and services providers. It scares off many businesses from using Blockchain technology.

Challenges: focus on Privacy

CyfRA

Blockchain as a distributed ledger **provides data transparency** by sharing the same documentations to all participants. There is an inherent trade-off between privacy and transparency.

Provision 4.8

Consumers who gave consent for the processing of their personal data shall be given the **opportunity to withdraw** it at any time. Data should be processed in accordance with applicable data protection law (**GDPR)**, and legislation.

Provision 4.11

Make it easy for consumers to **delete personal data** with clear instructions on how to do it.

This is not possible on Blockchain because of:

Immutability

Any data modification must be verified by the majority of the network nodes, therefore, Blockchain efficiently protects transactions but doesn't allow to erase personal sensitive data.

Possible mitigation solution:

Private Blockchain

all the participants are known and trusted. Is useful when the blockchain is used between companies that belong to the same legal mother entity and elaborate particular information

Smart contracts among things

Given the properties of the Blockchain is one of the key technologies that can securely enable **smart contracts among the “things”**.

Smart contracts are ***automatically carried out when a specific condition is met****, for instance regarding the conditions of goods or environmental conditions* or other smart applications that support specific Internet of Things processes.

That is, **smart devices** can **interact** and **transact with each other autonomously without human interventions.**

The blockchain will enable **autonomous smart devices to exchange data**, or even execute financial transactions, without the need of a centralized broker. This type of autonomy is possible because the nodes in the blockchain network will verify the validity of the transaction without relying on a centralized authority.

A **distributed model** is more efficient, secure, affordable, and will unlock even unforeseen residual benefits for IoT that have yet to be predicted

Conclusion

THANKS FOR YOUR ATTENTION