What is IOT?

The Internet of Things (IoT) describes the network of physical objects things that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. These devices range from ordinary household objects to sophisticated industrial tools. IoT has become one of the most important technologies of the 21st century By means of low cost computing, the cloud, big data, analytics, and mobile technologies, physical things can share and collect data with minimal human intervention.

**Threats to IOT security:**

A number of high-profile incidents where a common IoT device was used to infiltrate and attack the larger network has drawn attention to the need for IoT [security](https://searchsecurity.techtarget.com/definition/security). It is critical to ensuring the safety of networks with IoT devices connected to them. IoT security, includes [a wide range of techniques](https://internetofthingsagenda.techtarget.com/tip/Five-key-elements-of-securing-IoT-in-the-enterprise), strategies, protocols and actions that aim to mitigate the increasing IoT vulnerabilities of modern businesses.

* A survey of 260 IT decision-makers confirms widespread use of IoT devices in national companies of all sizes and industries
* The majority of respondents considers the Internet of Things to be insecure or not very secure and prevention measures for securing IoT devices inadequate
* The survey highlights unclear responsibilities and insufficient measures for risk prevention in the majority of companies. Specific risks of attack against IoT devices are underestimated[1]

**SECURITY REQUIRED TO ACHIEVE:**

#### Introduce IoT security during the design phase

Of the IoT security issues discussed, most can be overcome by better preparation, particularly during the research and development process at the start of any consumer-, enterprise- or industrial-based IoT device development. Enabling security by default is critical, as well as providing the most recent operating systems and using secure hardware.

#### PKI and digital certificates

Using a two-key asymmetric cryptosystem, PKI is able to facilitate the encryption and decryption of private messages and interactions using digital certificates. These systems help to protect the clear text information input by users into websites to complete private transactions

#### Network security

Using antimalware, firewalls and intrusion detection systems/intrusion prevention systems; blocking unauthorized IP (Internet Protocol) addresses; and ensuring systems are patched and up to date.

* **Network access control.**

 NAC can help identify and inventory IoT devices connecting to a network. This will provide a baseline for tracking and monitoring devices.

* **Segmentation.**

 IoT devices that need to connect directly to the internet should be segmented into their own networks and have restricted access to the enterprise network. Network segments should be monitoring for anomalous activity, where action can be taken, should an issue be detected.

* **Security gateways.**

 Acting as an intermediary between IoT devices and the network, security gateways have more processing power, memory and capabilities than the IoT devices themselves, which provides them the ability to implement features such as firewalls to ensure hackers cannot access the IoT devices they connect.

# What is blockchain?

Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant’s ledger. The decentralised database managed by multiple participants is known as Distributed Ledger Technology (DLT). Blockchain is a type of DLT in which transactions are recorded with an immutable cryptographic signature called a hash. This means if one block in one chain was changed, it would be immediately apparent it had been tampered with. If hackers wanted to corrupt a blockchain system, they would have to change every block in the chain, across all of the distributed versions of the chain.

# How Blockchain Could Revolutionize The Internet Of Things

Security of Internet of Things (IoT) devices is an ongoing problem. The largely unregulated IoT market leaves plenty of room for device hacking.

While there are many security recommendations for IoT devices, such as biometrics and two-factor authorization, one potential solution is blockchain IoT security. Blockchain, which is most familiar for bitcoin and Ethereum, offers an intriguing solution for IoT security. Blockchain contains strong protections against data tampering, locking access to Internet of Things devices, and allowing compromised devices in an IoT network to be shut down.[2]

* **Public access**

Blockchain is public, which means that it’s accessible to everyone in the network. All network participants can see the common history of stored blocks and transactions, but they need a private key to see the content. This gives a complete transparency to all operations and keeps data safe at the same time. Once a piece of information is stored on a blockchain, it is impossible to change it.

* **Secure data**

Blockchain uses advanced encryption algorithms to secure data, which makes it more private. This is done primarily for financial operations to be carried out without risks. Using the blockchain model, IoT devices may send and receive messages in the same way as financial transactions to enable secure data communication between connected things.

## BLOCKCHAIN MECHANISMS FOR IOT SECURITY

The application of blockchain in IoT security enables a direct information sharing between connected devices instead of communication via a centralized network, thus decreasing the susceptibility of IoT to cyber-threats.

Perhaps the most promising way of successfully combining the two technologies is to install chips in every IoT device.

Data no longer travels from sensors to the cloud to be approved, which single-handedly eliminates the possibility of the ‘man in the middle’ type of hacking attacks. Now the information is sealed by a private key directly on the device and is anchored in a public blockchain, which means that data about every access to a particular sensor is forever recorded on a ledger.

## Blockchain in IoT security: implementation challenges

IoT implies control over a network of devices, where multi-layered security has to be put in place.

One of the major roadblocks on the way to adoption is paradoxically linked to one of the proposed advantages of blockchain: every action on the network has to be approved by other network participants for it to go live. For example, in case of an obvious security breach through one of the connected devices, denying access to that device would significantly decrease the negative impact of spreading the malware. On a bigger scale, with thousands of ‘things’ connected to a large network, it can be difficult to receive consent from the majority of entities.

It could seem that this can at least be implemented for smaller systems like smart homes. Unfortunately, another challenge emerges: home devices don’t usually have enough computing power to maintain a blockchain.

There is no easy way to address this challenge, but a custom blockchain platform can be a solution. Blockchain developers have to ensure that corrupted devices could be instantly eliminated from the network without the need for a conventional blockchain consensus. Organizations should thoroughly investigate their privacy requirements and choose a proper blockchain type or request the development of a custom one until ready-made solutions appear on the mass market.[3]

FUTURE GENERATION COMPUTER SYSTEM

Future Generation Computer Systems is a monthly peer-reviewed scientific journal covering all aspects of computer engineering

in the field of computer science and computer systems, Future Generation Computer Systems has matured beyond its original aims and scope. Therefore it was decided to broaden the aims and scope especially towards the application of large computer systems being the domain of computational science research. The emphasis will now be on new, high quality, original work in the field of: New system architectures (among others for embedded computing) Resource management strategies Run-time support systems for advanced computing WEB and Internet based applications of computing Large-scale scientific and engineering computing (including HPCN) Modelling and simulation methods Advanced methods for data interpretation Complex system simulations New numerical algorithms New solver methods (particle methods, natural solvers etc.) In addition to the publication of original submitted material, the journal will continue the tradition of publishing special issues. These issues are completely dedicated to one specific topic considered to be of high relevance to the readership.[4]

REFRENCES:

**[1]** <https://www.iot-inspector.com/blog/iot-security-report-2021/?gclid=Cj0KCQjwnoqLBhD4ARIsAL5JedI134PZJe-6L2woqLQqf_wGUYe5fc3vnHzcJOXHxMGdkcXGA6dvLr0aAsjAEALw_wcB>

[2] <https://innovationatwork.ieee.org/blockchain-iot-security/>

[3] https://www.itransition.com/blog/blockchain-iot-security

[4] https://www.researchgate.net/journal/Future-Generation-Computer-Systems-0167-739X