Introduction:

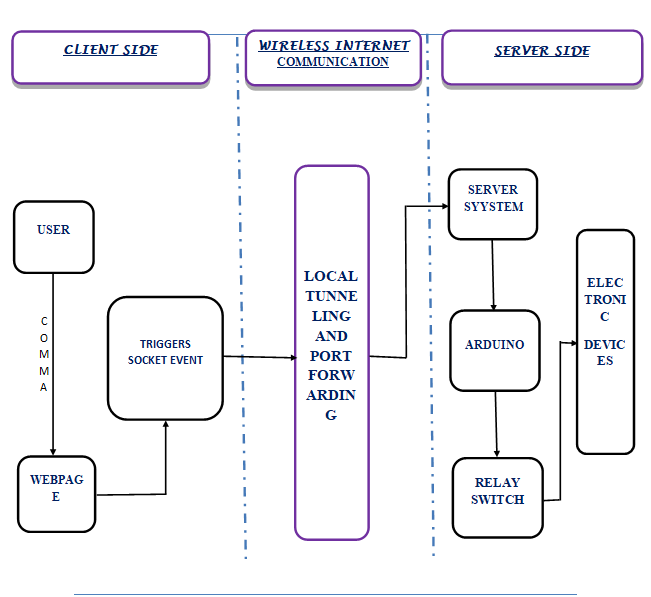
Contents:

* Description
* Iot
* Business insights
* Tunnelling protocol
* Tunnelling and Iot blocks
* Ai + tunnel = smart tunnel
* Why cloud is not suitable for Iot
* Case study 1:medical field and Iot block tunnelling
* Environmental engineering
* Case study 3: commercial appliances
* Conclusion

Description:

Webify is an IOT (Internet Of Things) project that aims to create an alternative cost effective solution to connect IOT devices to the cloud. The idea used is local tunnelling which provides the capability to the IOT device to connect online without any Internet drivers connected directly with the device. This simple alternative will save several thousands of money for large enterprises that are investing in IOT because the core of IOT (connection through internet) becomes simplified.

Existing IOT models use cloud systems like Google cloud platform, Amazon Web Services Microsoft Asure, IBM Watson, Losant for their IOT connection. These are not much reliable and providing our devices to the cloud is not reliable and may lead to a monocratic data dependent society. Thus local tunnelling our devices and maintaining a ledger for the connected devices will be more democratic and will be a better solution and also prevents us from relying on IaaS (Infrastructure as a Service ) providers like AWS. This solution is similar to torrents. Also it is estimated that by 2020, about 30 billion IOT devices will be online and the IOT enterprise business will sum up to a net total of 7.1 trillion dollars. Therefore this idea will have a bigger impact on the business economics if implemented.



IOT:



The **Internet of things** (**IoT**) is the network of physical devices, vehicles, home appliances and other items that can exchange data. Each thing is uniquely identifiable through its embedded computing system .Experts estimate that the IoT will consist of about 30 billion objects by 2020. It is also estimated that the economy of IoT will reach $7.1 trillion by 2020.

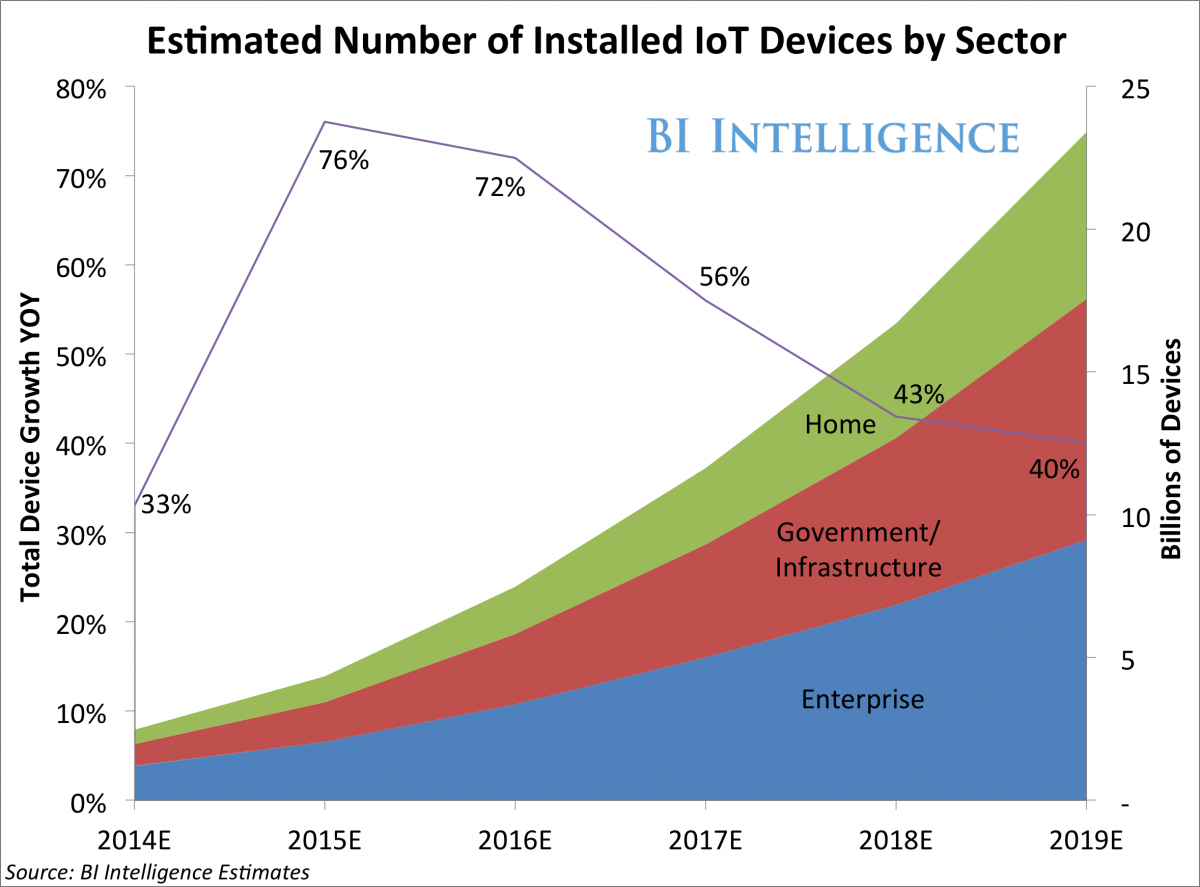
The IoT allows objects and physical devices to be sensed or controlled over the internet, creating opportunities for more direct integration of the physical world into computer-based systems. This makes Iot to be more relevant in a variety of future concepts like smart homes, smart vehicles.

Iot connects devices like household electronics, water transponders on farms, animal health monitors, cameras streaming live feeds of wild animals in coastal waters, automobiles with built-in sensors, DNA analysis devices for environmental/food/pathogen monitoring, or field operation devices that assist fire-fighters.

These devices collect useful data and flow the data between other devices.

The term "the Internet of things" was coined by [Kevin Ashton](https://en.wikipedia.org/wiki/Kevin_Ashton) of [Procter & Gamble](https://en.wikipedia.org/wiki/Procter_%26_Gamble), later [MIT](https://en.wikipedia.org/wiki/Massachusetts_Institute_of_Technology)'s Auto-ID Center, in 1999

BUSINESS INSIGHTS:



* [**The Internet of Things will be the largest device market in the world**](https://intelligence.businessinsider.com/the-internet-of-things-is-rising-examining-the-internet-of-things-2014-9?utm_source=House&utm_medium=Edit&utm_term=I-HUGEIoT-2014-10-9&utm_content=link&utm_campaign=BIIMobile)**.**We estimate that by 2019 it will be more than double the size of the smartphone, PC, tablet, connected car, and the wearable market *combined.*
* [**The IoT will result in $1.7 trillion in value added to the global economy in 2019**](https://intelligence.businessinsider.com/the-internet-of-things-is-rising-examining-the-internet-of-things-2014-9?utm_source=House&utm_medium=Edit&utm_term=I-HUGEIoT-2014-10-9&utm_content=link&utm_campaign=BIIMobile)**.**This includes hardware, software, installation costs, management services, and economic value added from realized IoT efficiencies.
* [**Device shipments will reach 6.7 billion in 2019 for a five-year CAGR of 61%**](https://intelligence.businessinsider.com/the-internet-of-things-is-rising-examining-the-internet-of-things-2014-9?utm_source=House&utm_medium=Edit&utm_term=I-HUGEIoT-2014-10-9&utm_content=link&utm_campaign=BIIMobile)**.**Revenue from hardware sales will be only $50 billion or 8% of the total revenue from IoT-specific efforts, as software makers and infrastructure companies will earn the lion's share.
* [**The enterprise sector will lead the IoT, accounting for 46% of device shipments this year**](https://intelligence.businessinsider.com/the-internet-of-things-is-rising-examining-the-internet-of-things-2014-9?utm_source=House&utm_medium=Edit&utm_term=I-HUGEIoT-2014-10-9&utm_content=link&utm_campaign=BIIMobile)**,**but that share will decline as the government and home sectors gain momentum. By 2019, government will be the leading sector for IoT device shipments.
* [**The main benefit of growth in the IoT will be increased efficiency and lower costs**](https://intelligence.businessinsider.com/the-internet-of-things-is-rising-examining-the-internet-of-things-2014-9?utm_source=House&utm_medium=Edit&utm_term=I-HUGEIoT-2014-10-9&utm_content=link&utm_campaign=BIIMobile)**.**The IoT promises increased efficiency within the home, city, and workplace by giving control to the user. However, many are hesitant to use devices as security problems are still an issue.
* [**The IoT lacks a common set of standards and technologies that would allow for compatibility and ease-of-use**](https://intelligence.businessinsider.com/the-internet-of-things-is-rising-examining-the-internet-of-things-2014-9?utm_source=House&utm_medium=Edit&utm_term=I-HUGEIoT-2014-10-9&utm_content=link&utm_campaign=BIIMobile)**.**There are currently few standards (or regulations) for what is needed to run an IoT device. Consortia that group together global industrial, tech, and electronics companies are involved in an effort to standardize the IoT and solve the most pressing security concerns.

Tunneling protocol

In computer networks, a **tunneling protocol** allows a network end user to access network service that the network does not provide directly. One important use of a tunneling protocol is to allow a foreign protocol to run over a network that does not support that particular protocol. Another important use is to provide services that are impractical or unsafe to be offered using only the underlying network services. Because tunnelling involves repackaging the traffic data into a different form, perhaps with encryption as standard, a third use is to hide the nature of the traffic that is run through the tunnels.

Tunnelling and Iot Blocks

The tunnelling technology is the most promising but unexposed technology that deserves some huge attention especially in the field of Iot. Tunnelling makes several initialization steps in the Iot platform unnecessary. The promise of this technology is that the internet will not influence iot and so physical devices won’t be hacked and they are secure. At the same time they are robust enough as they are backed up by existing protocols.

This technology also has the potential to create private Iot blocks in the internet that can communicate with each other and they could share relevant data between themselves. This would automate several tasks within the Iot block.

Iot blocks are a kind of yet to come idea that will glue up several physical objects inside a specific area and monitored by a man power or an AI. This kind of blocking up of the physical devices provide the necessary security and also the limit that any device could access data from.

Tunnelling makes this process of Iot Blocking possible by creating a tunnel for all the devices inside the block. Tunnels could possibly share certain amount of data. The level of data abstraction that every tunnel shows depends upon the need for data. Thus tunnels could make the entire Iot world private and separated from the vision of hackers.

In the enterprise level Iot blocks could be monitored individually using separate monitors. These monitors could also have the power to change and organise the level of data abstraction that every Iot block should show up to the immediate tunnel.

The monitoring of data is made possible by using tunnelling the data through a global server once for a required period of time. This kind of exposure of data may result in a security breach. So during the time of tunnelling the data to a central server, all the Iot blocks connected to the tunnel shouldbe disconnected just to prevent any control hijack by any anonymous user.

The monitors which are used in the central server may be human or AI or both and is capable of performing analytics of the data that was received from the tunnel. By the analyzed result we could make some useful outcomes of the resources.

For example,

If the analysis of a hospital Iot block shows that it used only 60% of the devices connected to the tunnel, then the administrator could remove unnecessary overhead in the tunnel.

Thus tunnelling of a Iot block proves to be a private and secure solution for implementation of Iot.

Tunnels also reduce the risk of cloud dependency of the physical world.

Thus they make everyone democratic and responsible for their Iot block.

Cloud dependency also increases the risk of exposure of Iot block to the rest of the world. This is reduced greatly by using tunnels.

Locally created tunnels are entirely responsible to the enterprise that created it. So this creates true ownership of the Iot device in the same way physical devices are truly owned now.

Ai + tunnel = smart tunnel!

Due to the rapid advancement of artificial intelligence and other soft computing technologies, Iot could rapidly utilize this technology.

Ai could make smart tunnels using deep neural networks that adapt to the analytics results of the Iot blocks. Artificially intelligent machines could compare several best possible tunnel paths and choose the best among them. This reduces the business cost for establishing Iot. This kind of tunnelling can be eventually termed as smart tunnelling.

Smart tunnelling solutions will greatly reduce the cost of establishment of tunnels across the physical world, because the need for checking all the devices manually and connecting them manually to the tunnel can be a cost and effort heavy process.

This effort heavy process can be greatly reduced by the usage of Artificially intelligent systems. Thus it can sense smartly and connect devices to the tunnel whenever needed.

This reduces the tunnel payload and unnecessary exposure of unused devices. This safe guards the devices from security hijacks.

The third use of Ai in Iot would be smart security to physical devices. Only the respective tunnels can access and share the data. Other tunnels are denied to access the data by using Ai security rules.

Thus Iot relies heavily on Ai to establish a true smart future that behaves and interacts the same way as it does today.

Why cloud is not suited for iot?

Existing Iot solutions use cloud computing technologies like amazon web services or IBM to connect their Iot devices online.

This is obviously a bad solution because of several reasons.

The first reason is that extreme cloud dependency may lead to a monocratic and dependent society which is obviously not expected by our future generations. Monocracy may prove wrong at times like it did in the ancient histories. Because Iot is such a huge data, we must not expose those data to a central authority. Also the world is now a days moving to a open sourced nature from a closed nature. This obviously is not supported by a monocratic society.

If any catastrophies occur in the central cloud servers, all the dependent Iot blocks would be suffered because they have no other way than to rely on the cloud providers.

The second reason is that all the resources get dumped up somewhere which may also prove to be a security issue. Hackers and security hijackers could easily find ways to steal and take over controls of the physical world.

This is a serious problem because Iot will be fitted even to hospitals. Thus if bad minds take over the control, they might result in a catastrophic situation.

The third reason is that cloud systems are costlier to establish and deploy.

An average amazon web services cost is around $100/month. It is really bad that we have to pay for them in order to control our own devices.

Case study 1: Medical field and Iot block tunnelling

Iot devices could become extremely important in the future of medical computing devices. This advancement is accompanied by artificial intelligence bots. Iot devices could be used in hospitals and other medical research areas to alert about the emergencies in the hospital. This could greatly be accompanied with tunnels so that it always creates a private Iot block.

In a busy hospital human resources alone cannot always make the best monitoring. Human made decisions are at times prone to errors. In a hospital these errors may lead to serious consequences.

So Iot devices combined with intelligent computers could make the best pair to monitor all the physical devices. The monitor could send a periodic interrupt signal to the tunnel which in turn may send the interrupt to all the physical devices.This is finally responded by the devices to the monitor.

The response should invlude the current status of the device. The hardware condition, The software condition and all other physical conditions of the device. This reduces unnecessary human technical resource.

Also artificial intelligence bot could gradually assist the doctors in the clinical treatments by analysing the conditions of the Iot blocks without any cloud and directly communicating with the device through tunnels.

Thus the entire technical management of the hospital is automated and it becomes an easy task for the doctors to do their job easily.

# Artificial pacemakers and their interaction:

Artificial pacemakers have been used in humans since a long time. If they could be tunnelled to the hospital then the doctors could gradually monitor the patient’s condition remotely. This also helps in emergency diagnosing of patients.

# ECG machines and their interaction:

Electro cardio gram machines used in the hospitals could be tunnelled and they could send periodic information about their condition and the patient’s heart condition. The results could be analyzed by a doctor and an artificial intelligence.

# Tunnelled dialyzer:

Dialyzers could be tunnelled to a central artificial intelligence and could monitored automatically by the machine and they could automatically refresh the dialyzers in the correct time.

There are several other applications of these kind of Iot blocks in the medical fields.

Other crazy application of this idea in the medical field is the brain computer interaction.

# Brain computer interaction:

Brain computer interaction is a upcoming technology that is yet to be exposed in the society. This technology implies the direct usage of our mind to control the computer.

If this technology becomes true then we humans could penetrate into our own tunnels and exploit the Iot blocks.

This idea will permanently change the way we interact with physical devices today.

Case study 2: environmental engineering

Iot devices could directly be used in environmental science and engineering technologies like solar panels, wind mills , geothermal energy extraction and many other renewable energy extraction fields.

Tunnelling the devices to the respective owners and inform them about their status and other conditions. This message should include details like current generation of energy , health of the physical devices etc.

The owner of the devices should also be able to communicate with the device through the tunnel and pass messages like reduce generation or turn off the device.

In the solar panels they could be embedded with other sensors like light sensor and the panels could orient themselves to the direction of light. This activity could be monitored by the AI.

Iot tunnels and Ai could change the shape of the windmills as per the orientation and power of wind.

Several shapes have been proposed for the orientation of windmills and the owner of the windmill cannot always predict the best shape for the mill. So an AI combined with the tunnel could actually grab the shape and compare it with the wind characters and predict the best shape.

Iot block concept could eventually be applied to a group of physical devices and they could be chosen wisely by the AI to match the climate needs.

All these kinds of process could not rely on cloud systems always and so tunnelling is important in these ideas.

Case study 3: Commercial appliances

In the third case Iot tunnels could be used in enterprise and households and other commercial business industries.

In the household Iot tunnels could be employed to directly control the physical devices over the internet.

In the business outsources they could be used as direct power supply resources.

These systems could be smartly controlled by intelligent machines over the internet as they could not be always monitored by human resources.

Businesses could charge commercials to provide services to tunnels.

By using these kind of tunnels in the household and commercial applications, we greatly reduce the overhead of manual monitoring of devices.

It can greatly save power and energy and make use of the existing energy efficiently.

Conclusion:

Thus the wide unexposed use of tunnelling have been discussed with several case studies. In order to make this vision possible, tunnelling technology has to come out commercially.

In the future, this technology may be even used in the brain computer interaction technologies to control physical devices with just thoughts! So the tunnelling technology has to be developed even further and exposed further to unlock it’s complete potentials.

Current tunnelling technologies are just in alpha or beta stage developments and not much commercially supported because of the limited exposure.

On the business and household side, this technology could be exposed to automate several tasks and control the physical devices from online over any distance, without any cloud dependency.

The final thought is that all data presently available should be open sourced and all future data also should not be dumped into a particular server. This will lead to a democratic online society for the future.

Thank you