Changing the game!

(I)IoT

Establishing a controlled and protected IoT, fullfilling even the highest industrial security demands.

1. Current Situation

All possible IoT scenarios are facing similar challenges – how to secure billions of different devices, network and server components? How to protect the data flows between all those components? How to ensure that only the desired parties will have access to the data? Since every single device is a possible attack point, each one must have a similar level of protection, whether it is an electricity meter or a nuclear plant. Rising complexity makes it virtually impossible to control and secure all connected devices, even if Edge of Fog computing scenarios add some form of segregation to build better manageable sub-groups.

2. Key Issues

a. Growing Complexity

Even though the predictions on the number of connected devices differ a lot, they have one thing in common – the numbers are huge. Billions of devices will be connected in our near future, long term almost everything will be connected and exchange data. Cars will become computers on wheels, houses will have more and more sensors, and this is and will also happen to us humans. Data will be everywhere.

There is a lot of benefit and value involved in this development, but also huge risks. Today's security technologies have never been invented to handle this complexity, as the build protection layers around the data (e.g. via encryption). However, this conflict between total connectivity and protective "walls" around objects or data can't be resolved with today's technologies. Therefore, only "workaround solutions" exist, which even add more complexity. We clearly see the results in data breaches in the news almost every day.

b. Massive risk increase

So far, most IoT solutions have been built in the B2C area, but this development is spreading fast into the B2B area. Even critical infrastructures like power generation facilities or hospitals are using more and more connected devices and even the cloud. In general, this is the right direction, as improved communication and increased knowledge will help our society a lot to grow, but due to the complexity explosion also the risks do explode. Those risks are not only financial risks but could even lead to massive harm (due to e.g. accidents of autonomous cars) or death (e.g. hacked medical devices), even for many humans (e.g. manipulated industrial facilities). Even cyber warfare will become more and more effective, and the involved parties more and more powerful. We urgently need to change this situation.

c. Data Ownership - Privacy vs. Openness

Data Ownership is a very ambivalent topic. In some countries the data regulation laws clearly state that the one who entered the data is also the owner. However, in reality the supplier of an application or service gathering the data has also the control of it, so it's required to trust that 3rd party to use the data solely to the agreed extend. Sharing any kind of information means today, that we need to trust the one we share information with, including the risk that (either intentional or unintentional) this information can be abused (as recent examples at Facebook or Twitter have shown). In bigger, more connected and heterogenous scenarios as the IoT, the privacy protection becomes even more complex, as more and more devices of various vendors are collecting (sensitive) data.

Surveillance laws or the ban of certain protection mechanisms (like VPN) complicate the privacy and secure data exchange topic even more, especially in the B2B area, where sometimes highly confidential information has to be exchanged, e.g. to be able to outsource parts of the supply chain / manufactory processes.

d. Heterogeneity

As almost every device will be connected in the future, also lots of different producers and types of devices will be involved. Due to the internet / cloud structure, point-2-point connections will be the exception, normally lots of different partners/devices/solutions will be involved (e.g. sensors, gateways, routers, servers, networks, protocols, etc.).

Currently lots of vendors and interest groups try to establish (I)IoT standards or "operating systems" grouping several IoT components (e.g. Microsoft, Siemens, GE, Samsung, Cisco, OpenFog, OPC etc.), but different goals and especially unsolved problems in the privacy and security area hinder establishing a common trusted (I)Iot standard yet.

e. Connecting Industrial Machines

Industrial machines differ a lot from typical computer devices in size, investment, and especially lifespan. Especially machines used in critical infrastructures need to be protected at the highest possible level. To limit the risks usually network segments are used or connectivity and data exchange is minimized, limiting the possible benefits of smart manufacturing. Even more critical than protecting the sensor information for the physical machines will be to protect the "digital-twins" build and the data gathered, as this information provides deep insights into the business processes, differentiation and IP of a company – and even enables a company to simulate the production changes and enhancements of the future. Those twins will become a major asset of every company and needs to be protected accordingly.

3. NVD (Non-visible-data Technology) advantages for the IoT

Non-Visible-Data Technology has been built to provide a solution to store and exchange data with full privacy and control in heterogenous and highly distributed connected environments like the IoT. Highest scalability and performance with minimized overhead and resource needs have been targeted from the very beginning. Any kind of binary information (data) will be automatically converted to NVD-data blocks already during the data creation, ensuring that the data content is protected along the full data lifecycle.

a. Simplification driving down cost

NVD massively reduces the complexity of building and maintaining secure (I)IoT solutions. Due to the integrated protection within the data, no additional protection is required (secure networks, routers, servers etc.), and even already shared data can be actively revoked at any time. No complex design is needed (which parties are allowed to access which data, how critical is the shared information, what protection mechanisms and technologies are required to protect the data etc.). Maintenance is made simple, as no external and even internal admin is having any insight or access into the data content.

NVD also replaces the key management and -storage, one of the main weaknesses of todays' security solutions (esp. in regard to scalability). As no key vault is required, the risk of compromised keys is eliminated.

b. Digital Immunity

NVD technology ensures that data on all devices is made immune to attacks or manipulation. This is achieved by applying an extremely efficient procedure right when the data is first created, providing a permanent protection – which makes it completely irrelevant if data later is stored or transferred on insecure or even compromised devices.

NVD not only solves the challenges described, but vastly simplifies and reduces the complexity of IoT architectures, since immediate protection eliminates the complex need to secure every single device in the chain.

c. Guaranteed Privacy and active data revocation

With NVD privacy and openness can be balanced, as the data control is given back to the owner who created the data. Immediate protection ensures that no (untrusted) party has access to the data, and due to the build-in active revocation features even pre-shared information can be revoked later if needed, so sharing "mistakes" can be undone.

d. Data Control instead of need to trust

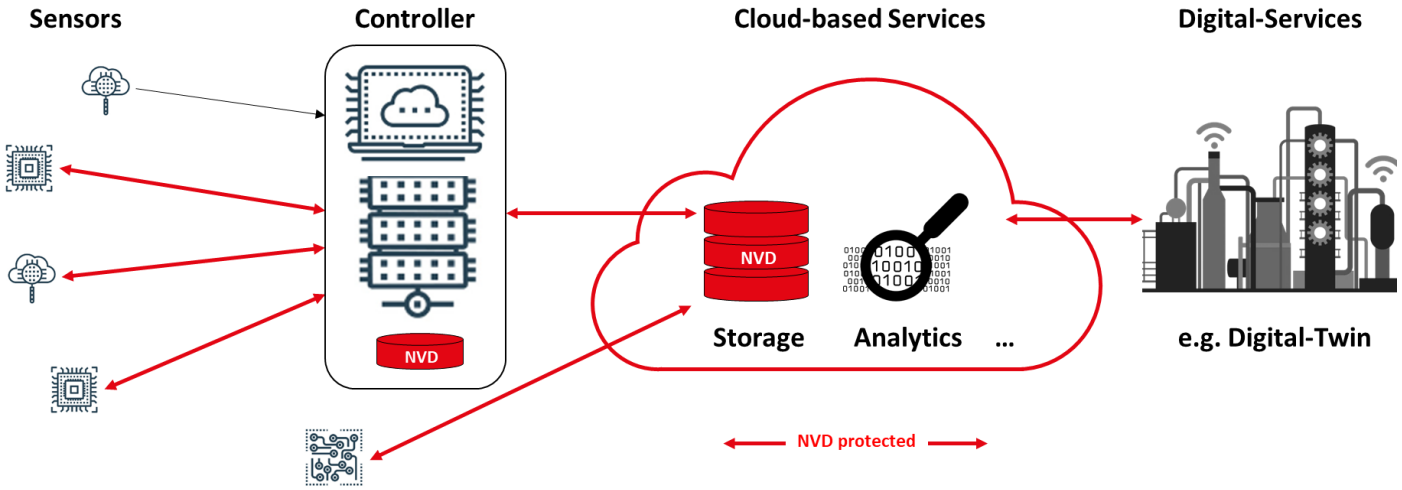
With NVD it doesn't matter how many different parties will be involved, or how many devices might have access to the data (e.g. routers during the transmission process). As the NVD data is protected from the beginning, and includes no information about content, owner, access-rights etc. (meta-data) it can be transferred and stored without the need to trust any device or party which has access to NVD. NVD has been developed to run on every device, even on simple embedded devices like sensors. Therefore, it provides the ultimate protection on every device.

e. Invisible / Stealth Mode

Most of the industrial machines have not been designed to be integrated into connected environments and connecting them could mean unforeseeable risks. With NVD those machines can remain "invisible" from the outside, NVD even doesn't require an IP-address to operate. Nevertheless information/data can be exchanged highly secure and private without being visible by 3rd parties – which removes the risk of connecting those industrial machines.

4. NVD based IoT problem resolutions

NVD enhanced products can enable data protection already on sensor level, and along the full data lifecycle. The protected data ensures that the data control stays within the company, even in highly connected and distributed (cloud) environments. Due to the clear separation of data (platform) services as digital twins or analytics can be used without the risk of data abuse or manipulation, resulting in highly efficient and cost effective secure products.



a. NVD-based sensors

Depending on the chosen IoT architecture and sensor connectivity sensitive information might be distributed. Inbound traffic to control the sensor is even more critical and therefore often prohibited. NVD enabled sensors ensure best possible protection in both directions and with lowest possible overhead. As soon as a device is powerful enough to run encryption algorithms, it can also be NVD enabled. Since NVD doesn't require IP addresses, the sensors and the data could even kept invisible from others.

b. Highly secure controllers

In IoT scenarios like fog/edge computing or NB-IoT most sensors are not properly protected and protection starts within the (automation) controllers. NVD-based controllers could handle both the data of NVD sensors and provide highest data protection for the data stored in the controller and send to other entities – without the effort and cost necessary with current technologies (e.g. TPM modules, key management/vault solutions, secured network components etc.). Therefore, the cost for building NVD-based controllers would be significantly below todays' secure controllers but providing much better protection and performance with less overhead.

c. Joint IoT cloud storage

As the NVD-enabled hardware components already generated NVD, there is no need for highly protected or private cloud solutions. Cost for network and cloud services would be significantly lower compared to todays' solutions.

d. Service usage without lost data control

The access/referencing model of NVD ensures that data access can be linked to specific users, applications, processes, timeframes and even locations. Therefore, common services can be used ensuring that no unwanted 3rd parties get access to the data. Provider can guarantee that customers can use their services without them being able to see any information. This new level of control and privacy will help to massively increase the usage of common services.

5.Use Case Evaluation

The following evaluation analyses the suggested problem resolutions in regard to

a. the implementation complexity, probability, the needed extension of the NVD technology and the required implementation effort
b. quantitative (revenue increase or cost reductions) and qualitative (company image, compliance)
c. matching customer segments and target buyers

a. Implementation

Problem resolution	Implementation			
	Complexity	**Probability**	**Extension**	**Effort**
a) NVD-based sensors	Low	Medium	NVD integration into hardware	Medium
b) Highly secure controllers	Medium	High	NVD integration into hardware	Medium
c) Joint IoT cloud storage	Low	High	None	Low
d) Service usage without lost data control	High	High	Dedicated NVD based applications	High

b. Quantitative and qualitative assessment

Problem resolution	Quantitative advantages		Qualtitative Advantages		Customer segment	Target buyers
	Revenue increase	**Cost reduction**	**Image gain**	**Compliance**	IoT hardware & software vendors	Bosch, Cisco, Dell, Fujitsu, GE, Google, Huawei, IBM, Intel, Microsoft, Qualcomm, Samsung, Siemens
a) NVD-based sensors	Medium to High	Low	Medium	High		
b) Highly secure controllers	High	Medium	Medium	High		
c) Joint IoT cloud storage	Medium	High	Medium	High		
d) Service usage without lost data control	High	Low	High	High		