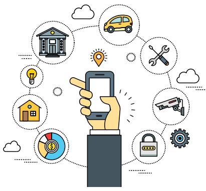


IoT Standards

IoT Standards will look at different segments of the IoT market as it relates to implementation and use of standards. Each column will select a particular vertical, and lay out the relevant standards and technologies that affect the evolving IoT hyperspace. The pace of the columns will start broadly with the vision of narrowing the subject of subsequent articles toward more specific applications of standards, whether in the development, application, test, or commissioning of IoT technologies.

Introduction

The new paradigm of smart home, smart building, smart grid, smart manufacturing, and smart city already complicated by the Internet of Things and the Internet of Everything made further complex by the 5G and (now 6G in the very near future), artificial intelligence, machine learning, blockchain, and quantum computing, make it truly complex to develop and embed comprehensive security, privacy, and trustworthiness attributes in the products, systems, and solutions for any use case or application — be it consumer, commercial, industrial, automotive, or strategic domains like critical infrastructure, defence, and aerospace. Now, Artificial Intelligence of Things (AIoT) brings further complications to security strategies due to exponentially multiplied nuances of IoT and AI paridigms who, in their individual right, have been well recognized as profound technologies as they are making themselselves invisible by weaving themselves into the fabric of everyday life until they becomes indistinguishable from it.

Mentor's Musings on Security Standardization Challenges and Imperatives for Artificial Intelligence of Things

by N. Kishor Narang
Technology Philanthropist, Innovation & Standardization Evangelist

The recent evolution of disruptive technologies and digitalization compounded by COVID-19, changing geopolitical situations, and increasing cyber-attacks from not-so-friendly nations, bring a whole new set of challenges for the security and security evaluation methodologies for the complex nature and architectures of critical infrastructures of nations leveraging the IT, OT, Internet of Things (IoT), and communication networks evolving to meet these rising needs of society.

On one hand, we have highly protected networks for the critical information infrastructures; on the other hand, these very highly protected networks need to give access to consumers for consumer engagement and participation in these digital infrastructures to meet the true drivers of setting them up. These large smart networks are actually highly complex Systems of Systems and Networks of Networks, and thus create fresh challenges in the security paradigm and development of security startegies.

Have we seen ALL that is involved in cyber security??? Those of us who have worked in cybersecurity for many years often start to think we have "seen it all." We have not. Recent years have ushered in a host of new adversaries, new attack methods, and new challenges for those of us in the cybersecurity industry.

It is evident that cyber security is a very complex paradigm, and with evolving new technologies, requirements, and ever-increasing attack surface, the vulnerabilities are rising many folds over time. In such a dynamic scenario, how do we develop a cyber security strategy to make our critical infrastructure comprehensively safe, secure, resilient, and trustworthy?

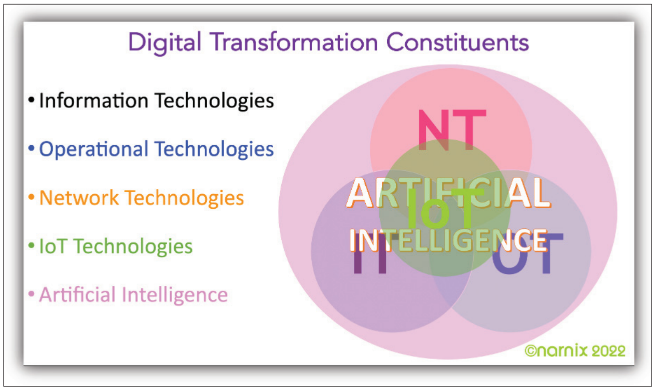
The critical infrastructure and even otherwise cyberthreat vulnerability landscape is rapidly evolving and expanding, with more frequent attacks, more numerous and varied threat actors, and increasingly sophisticated malware and tools that are more widely available and sometimes indiscriminately deployed. Critical infrastructure operations are among the most frequently attacked targets, increasingly by nation-state actors aiming for disruption and even destruction through industrial control system (ICS) and IoT devices.

Digital Transformation

Society, business, infrastructure, services, and all other aspects of civilization on planet Earth are going through a paradigm shift in the wake of technological advancements, especially in the field of ICT. All ecosystems, be they smart cities, smart grid, smart buildings, or smart factories, now find themselves making three classes of transformations:

- Improvement of infrastructure — to make it resilient and sustainable
- Addition of the digital layer — which is the essence of the smart paradigm
- Business process transformation — necessary to capitalize on the investments in smart technologies

The genesis of digital transformation in any paradigm, domain, or ecosystem: Sustainability is the true destination, resilience is the core characteristic, smart is merely the accelerator, and standards are the chromosomes of digital infrastructure.



Digital Transformation Constituents

- Information Technologies
- Operational Technologies
- Network Technologies
- IoT Technologies
- Artificial Intelligence

Digital transformation is NOT a technology. It is a complex paradigm with domain-specific implications as we are living in an ephemeral world, and artificial intelligence (AI) and machine learning (ML) are powering the digital transformations happening in every industry around the world.

Demystifying AIoT

IoT and AI, which both individually originally sounded like something out of sci-fi movies, are in fact reality, and are bound to become even more widespread. From being considered as some of the most disruptive technologies since the World Wide Web to being on the verge of becoming some of the most profound technologies by *weaving themselves into the fabric of everyday life, until they becomes indistinguishable from it*[1]...

New technologies and paradigms like IoT, big data, AI, virtualization, 5G/6G, AR/VR, cloud and edge computing, Web

3.0, and metaverse are promising to disrupt the way we design products, systems, and solutions. Design engineers need to develop new strategies that can help them navigate seamlessly through a much wider and complex canvas of technologies, ecosystems, and stakeholders. However, it is difficult for innovation to happen across disjointed platforms and technologies. Creating the opportunity for ecosystem partners to work across common open platforms facilitates faster innovation.

AIoT stands for Artificial Intelligence of Things; it combines the connectivity from IoT with the data-driven knowledge obtained from AI. This emerging technology is based on the integration of AI in IoT infrastructure.

By combining IoT with AI, the data collected by distributed nodes can be utilized by applying AI techniques such as ML and deep learning. As a result, ML capabilities are moved closer to the data source. This concept is called edge AI or edge intelligence, and it allows higher scalability, robustness, and efficiency. The combination of the two concepts (AI and IoT) focuses on using AI capabilities to process the data generated and collected by IoT systems. Therefore, ML models in AI systems are combined with the connectivity and data transfer capabilities of IoT. In other words, with the incorporation of AI in IoT systems, their functioning is not limited to collecting and transferring information but actually understanding and analyzing the data.

AIoT is a new trend that combines AI with IoT to create networks of digital devices that communicate and process data. While IoT creates vast connections, AI makes these devices come alive. Here is one example: an IP camera system can be used for apartment security. However, without AI, people need to monitor video from the system in real time in order to respond to emergencies. With AI, IP cameras can recognize risks automatically and send alerts.

Certainly, AIoT promises to grow rapidly and give rise to new high-value products in the same way that the Internet led to the creation of so many huge businesses. Those who enter the production of AIoT devices will be poised to tap a vast new market. IoT devices today number in the billions. These small, connected gadgets include electronic devices and appliances networked together and communicating over Internet Protocols (IP).

In IoT, we connect intelligent products and services, generating added value for our customers. By adding AI, we create a closed value creation cycle and focus even more on users. The data resulting from the use of intelligent, connected products and the interaction between people and machines and machines themselves are the key factor in this context. By linking IoT with AI and ML, we can draw the right conclusions from huge quantities of data and react to these data during product engineering in seconds. We learn from the data, and thus can improve our products and services on an ongoing basis.

AIoT makes it possible to develop new products more quickly. At the same time, we can optimize customers' products during their lifetime (e.g., by using over-the-air updates) or add new functions. By using data as a basis for optimizing and personalizing our products, the need for privacy and AIoT security grows. The greater people's trust in AIoT, the greater their acceptance.

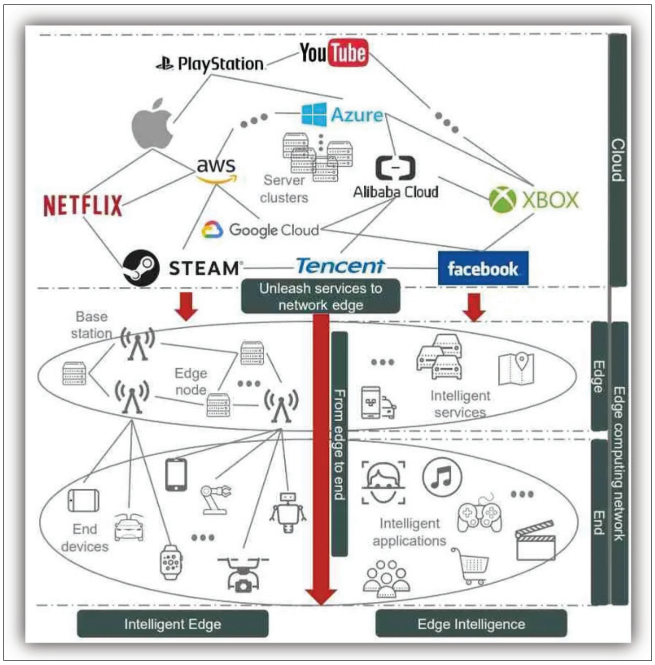
In recent years, the edge computing paradigm has gained considerable popularity. It serves as a key enabler for many future technologies like IoT, 5G, and AI. Hence, edge computing is the primary driver of AIoT; it moves data processing from the cloud to the network edge.

AIoT combines the power and efficiency of both AI and IoT, making it suitable for solving specific problems with distributed, intelligent systems. From retail to manufacturing, healthcare, security, banking, and insurance, the number of industries turning to AIoT powered solutions is rapidly increasing. In all probability, the technologies are all set for further advancement in the near future.

Shaping the transformation: the use of AI within IoT. The COVID-19 pandemic, climate change, and digitalization have changed people's needs and desires. The focus is now on health, sustainability, and data security. In order to cope with this rapid transformation and respond in a customer-centric manner, combining AI and IoT in AIoT is proving to be immensely useful.

Edge-Computing-Powered Artificial Intelligence of Things

The concept of edge computing promotes distributed system designs with on-device data processing that is highly efficient, scalable, robust, and suitable for low-latency use cases. Initially, ML and deep learning were limited to the cloud, mainly because of the availability and scalability of the high computational resources required to process ML tasks. By exploiting the novel paradigm of edge intelligence, emerging computational intensive and resource-demanding AIoT applications can be efficiently supported at the network edge. Therefore, edge computing is essential to achieve the fast processing capacity and low latency required in intelligent IoT applications.



On-Device Machine Learning with AIoT Devices

The recent advances in hardware and ML have accelerated the deployment of billions of interconnected, intelligent, and adaptive devices in critical infrastructures like health, environmental control, logistics, transportation, and agriculture. Moving the AI processing from the Cloud to distributed, connected edge devices provides a solution to overcome the bottlenecks, latency, and privacy issues of cloud-based AI applications.

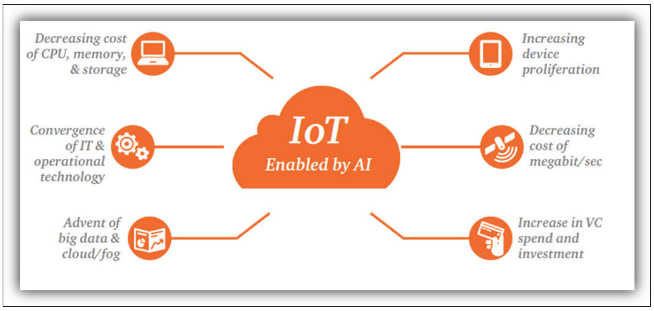
Compared to traditionally low-powered IoT devices, AIoT demands edge devices with sufficient computing resources to perform on-device machine learning tasks. However, the resource capacity and power budget of edge devices are naturally limited. As a result, AIoT applications are based on an optimization challenge to balance hardware cost and performance with an optimized AI model and application design.

This is the reason why recent trends focus on AI model optimization to minimize the model size and find ways to increase the model efficacy. AI model compression is used to implement low-latency and energy-efficient model inference at the edge. The much smaller and more efficient "lightweight" ML models can run on low-power devices like mobile phones, system on chip (SoC), or embedded computers. Popular examples are on-device ML model versions TensorFlow Lite or Lightweight OpenPose.

Embedded ML on-device transforms AIoT devices into smart, intelligent systems that can process data independently. The technical advances in different fields make it possible to apply AI technology efficiently. The newly gained flexibility and scalability of AIoT systems allow building real-world applications that have not been possible before.

Benefits of Combining AI with IoT

AIoT enables AI adoption across industries to solve real business problems more effectively than with traditional methods. There are several benefits of combining AI with IoT, the foremost being improved efficiency and reduced costs.


Decreasing cost of CPU, memory, & storage
Increasing device proliferation
Convergence of IT & operational technology
IoT
Enabled by AI
Decreasing cost of megabit/sec
Advent of big data & cloud/fog
Increase in VC spend and investment

Boosts Operational Efficiency by Continually Improved Decisions: AIoT enables businesses to achieve the optimum level of operational efficiency. AIoT-powered machines are capable of generating and analyzing data and recognizing patterns by applying ML methods. This enables it to provide operational insights quickly, detect and fix problems, as well as to increase automation of manual processes. Hence, AI capabilities performed on repetitive tasks enable companies to provide better services with a smaller workforce.

An example is the automation of vision-based quality inspection and the use of cameras for quality control in industrial automation. Various applications aim to track and ensure adherence to guidelines and regulations (e.g., detecting personal protective equipment such as masks, helmets, vests, and gloves). Devices like smart home devices collect personal preferences, which can be used in improving ML models. Using approaches like federated learning, AIoT devices can learn from user preferences and improve their decisions.

Makes Real-Time Monitoring and Operational Decision Making Easier: Real-time monitoring of systems can help save time and reduce expensive business interruptions. It involves constant supervision by the system to detect anomalies and make predictions or make decisions based on the same. Also, this is done without the need for any human intervention, achieving faster, objective results. An example is the use of industrial AIoT in oil and gas, such as cameras for remote leakage detection. Therefore, AIoT technology moves decision making from the human to the IoT device, enabling labor savings and improved compliance.

Reduces Operational (Data Transfer) Costs: Intelligent AIoT devices and systems play an essential role in reducing operational costs. Keeping AI systems in central locations leads to significant data transfer between edge devices and central servers. AIoT systems move analytics to edge devices and minimize data transfer. The development of smart systems allows higher resource efficiency. Examples include smart building applications for adjusting light and temperature controls based on occupancy (presence of people). AIoT devices play a crucial role in preventive maintenance and machinery analysis in smart factories. Here, sensors and cameras identify and monitor the condition of machine parts to avoid failure and expensive business interruptions (smart factory applications).

Helps in Risk Management: Risk management is important for organizations across industries. Distributed, intelligent systems are capable of predicting future risks and even taking measures for their prevention. Examples include the analysis of water levels, employee safety analysis, and crowd analysis in public places (smarty city).

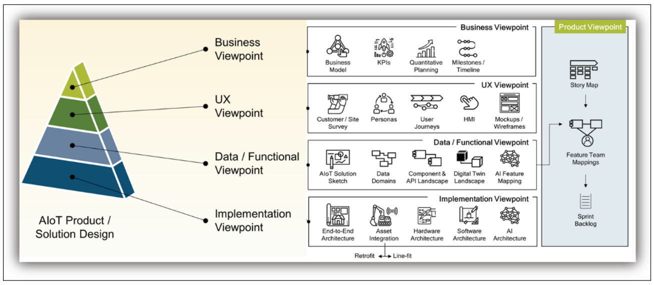
With the help of AIoT systems, organizations can stay a step ahead in preparing for and handling probable risks in the future. Recently, insurers started to use such applications to manage insurance risks for automobiles, machines, and entire factories.

AIoT Applications

Integrating AI with IoT is the basis of highly scalable and efficient intelligent systems that combine software and hardware. Hence, AIoT makes it possible to develop and maintain large-scale deep learning systems.

The adoption of AIoT is an emerging technology trend across a wide range of industries, such as automated vehicles, video surveillance, traffic monitoring, manufacturing and production, smart homes, smart buildings, smart grids, smart cities, wearable devices, autonomous things (AuT), Industrial IoT (IIoT), logistics, agriculture, healthcare, oil and gas, retail, and services. Specific applications in IIoT leverage AI capabilities in smart sensing, machine vision, and predictive maintenance.

AIoT Design Viewpoints

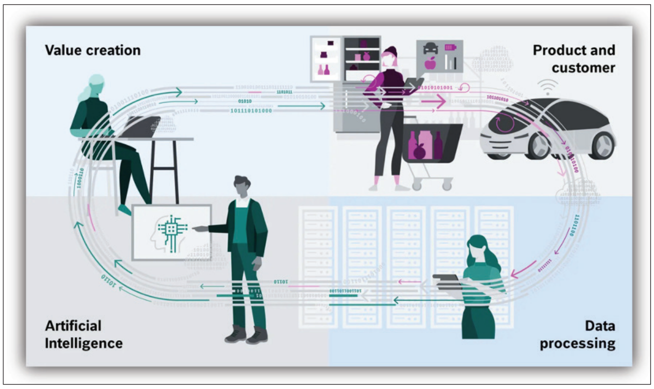


An important element in the development life cycle of AIoT is the end-to-end design of the product or solution. It is important to develop a set of detailed templates that can be aligned with the agile product development perspective, in particular the story map as the top-level work breakdown. To provide a consistent and comprehensive design for AIoT-enabled products or solutions, a set of design viewpoints are very helpful to get some structured understanding, each with a specific set of design templates:

- **Business Viewpoint:** Builds on the input from the business model, adds key performance indicators (KPIs), and planning details
- **UX Viewpoint:** Focuses on how users are interacting with and experiencing the product or solution
- **Data/Functional Viewpoint:** Focuses on the data and functional components of the AIoT solution
- **Implementation Viewpoint:** Adds details on the implementation aspects
- **AIoT Product Viewpoint:** Mapping to the agile product development perspective

Develop, Connect, Improve: The AIoT Cycle

The so-called AIoT cycle — a value creation cycle comprising four phases — shows the benefits of linking AI and IoT.



Value Creation: Connected products provide data. Companies use these data during research and development to improve applications and revise or supplement functions. At the same time, they can improve the security and reliability of their products on an ongoing basis and adapt them to meet the individual needs of customers. Making AI in AIoT products secure, robust, and explainable is a key issue for this. Research projects such as ML testing and AI safety help to achieve this goal.

Products in Interaction with Customers: Quite a many companies today deliver connected products and services to their respective customers. When these products are used, they generate data, which is used in the following phases of the cycle to improve products and applications. AIoT products ensure greater security for users. Research projects such as embedded AI based siren detection show this.

Data Processing: The data that are produced when connected products are used are the basis for this phase of the AIoT cycle. They are collected and stored in a structured manner. With technologies such as self-sovereign identities (SSI) and trustworthy computing, it can be ensured that users can keep control and maintain sovereignty over their data at all times and that these data are always protected.

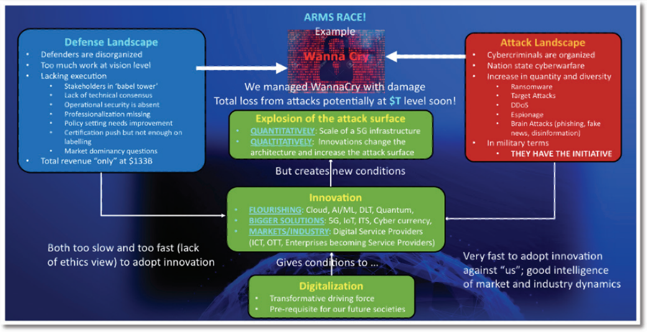
AI Algorithms: In this phase, the data is processed using AI algorithms and ML to gain new findings on this basis. The visual analytics research project shows how this process leads to greater security for users: in autonomous vehicles, AI is used for image recognition. In rarely occurring situations where several unusual conditions converge, so-called corner cases, the AI in the image recognition system points out weaknesses (e.g., when a red traffic light is hard to see from a certain angle in inclement weather). Visual analytics helps to detect blind spots and to automatically supplement the existing dataset with the help of a second AI. As a result, shortcomings of the first AI are remedied and overall system accuracy can be increased.

Securing the Future of AIoT

The Chain Is as STRONG as the WEAKEST Link

The proliferation of smartphones and mobile devices has benefited our society an immeasurable amount; their existence enriches and simplifies our lives. The convenience that comes with using smart devices, and IoT and AIoT is so ingrained in our society that we now take it for granted.

We have invested our trust in these devices. We store our schedules, contacts, and photographs on our phones; allow smart devices to control the lights and heating in our homes; smart cameras watch over our property and valuables; and smart speakers know what song we want next. We trust these devices with the most valuable commodity — our data.



ARMS RACE!

Example

Wanna Cry

We managed WannaCry with damage
Total loss from attacks potentially at $T level soon!

Defense Landscape

- Defenders are disorganized
- Too much work at vision level
- Lacking execution
  - Stakeholders in 'babel tower'
  - Lack of technical consensus
  - Operational security is absent
  - Professionalization missing
  - Policy setting needs improvement
  - Certification push but not enough on labelling
  - Market dominancy questions
- Total revenue "only" at $133B

Both too slow and too fast (lack of ethics view) to adopt innovation

Attack Landscape

- Cybercriminals are organized
- Nation state cyberwarfare
- Increase in quantity and diversity
  - Ransomware
  - Target Attacks
  - DDoS
  - Espionage
  - Brain Attacks (phishing, fake news, disinformation)
- In military terms
  - THEY HAVE THE INITIATIVE

Very fast to adopt innovation against "us"; good intelligence of market and industry dynamics

Explosion of the attack surface

- QUANTITATIVELY: Scale of a 5G infrastructure
- QUALTITATIVELY: Innovations change the architecture and increase the attack surface

But creates new conditions

Innovation

- FLOURISHING: Cloud, AI/ML, DLT, Quantum,
- BIGGER SOLUTIONS: 5G, IoT, ITS, Cyber currency,
- MARKETS/INDUSTRY: Digital Service Providers (ICT, OTT, Enterprises becoming Service Providers)

Gives conditions to ...

Digitalization

- Transformative driving force
- Pre-requisite for our future societies

Cyber security ecosystem.

With the number of IoT and AIoT devices expected to increase by such a huge percentage, we need to answer the question of security. As much as our lives have been improved by smart devices, IoT, and AIoT, there have been countless reports in the media of smart devices in homes that have been breached. When a device has been breached, it can act as an open door into the user's life, allowing perpetrators to gain access to anything from the mundane, such as your smart bulbs, to those devices you need to have bulletproof security: cameras, speakers, and even locks.

The AI in smart devices is what allows the device to learn our schedule, recognize our faces, suggest films, and much more. Most devices utilize a cloud connection only to run AI applications and access the databases they require to function, as the cloud provides an easy way to access necessary storage and processing power.

For many years, using cloud services was the go-to option for consumers and businesses, as the ease of access that the cloud offered was unrivaled. Recent, and frequent, security and privacy breaches have left many questioning if utilizing cloud storage on its own is still the only solution, and if privacy breaches are just the cost of using these devices.

Security concerns remain the number one asterisk for cloud computing. There have been many publicized cloud breaches. From personal information, employees' login credentials, to losses of intellectual property, once data is stored off the device, there is a security risk.

In cloud computing, the question of ownership of data is one that many companies and consumers have struggled with. Data and encryption keys reside within your third-party provider, so if the unexpected happens and there is downtime, you may be unable to access that data. If this happens it could mean that the facial recognition camera that allows you access to your home won't automatically open the door.

Distributed denial-of-service (DDoS) attacks are already prolific and highly disruptive. Some of the services that have become so ingrained in our lives are at the mercy of bad actors at any time. With 41.6 billion IoT devices expected to be online in 2025, the resources for DDoS attacks will effectively double.

The current amount of data that needs to be transferred to the cloud for processing is huge and will only continue to grow as our reliance on cloud services grows. This will exponentially increase our bandwidth needs and the associated costs to store and compute everything in the cloud. In the end, the high costs will be passed down to consumers.

On-Device Edge AI: On-device edge AI processing is a way of augmenting the use of cloud. Its addition allows data to be processed and inferred locally on the device, and it does not need to leave the device for the applications to work. As a result, massive amounts of data do not need to constantly be sent to and stored on servers run by big tech companies or governments.

Instead, most data will have been computed on the device, allowing for most data to be deleted, while only significant data that requires confirmation of action will be saved and sent to the cloud to be processed for further action. It is the most secure and private way of operating business applications, and significantly cuts down on costs associated with higher bandwidth needs and cloud storage.

In the past, chips quickly became outdated, but on-device technology is at a point where the chips being used are reconfigurable, meaning they can adapt to upgrades and developments in AI technology and adjust to the AI models of the future. Essentially, by breaking AI models down into basic building blocks, they can be reconfigured easily to take advantage of next-gen software enhancements. Hence, if AI technology sees a major update, the chips can be updated in the same device, rather than a whole replacement needed.

If on-device processing is adopted across the board, it has the power to create the most secure and private environment/network available to connect every AI/smart device and service in a user's life. Rather than devices reporting back to the cloud, devices will instead talk to each other in a private network. This will enable seamless, secure, and private use of all AI that will enhance people's lives.

Hybrid Solution: To completely abandon the cloud and rely solely on on-device processing would be to make the same mistakes as developers did in the past. It is not a choice between cloud and on-device; instead, we should aim to have cloud and on-device work in tandem and complement each other.

The security and privacy of on-device combined with the vast storage and processing power of the cloud will shape the next generation of smart devices and IoT. This hybrid solution will allow AI to reach its full and true potential. The promise of a fully connected society, powered by advanced on-device chips and supported by robust clouds, is closer than ever before. With the right technical implementations, we can enrich our lives and take another step forward into the future.

The Challenges of AIoT

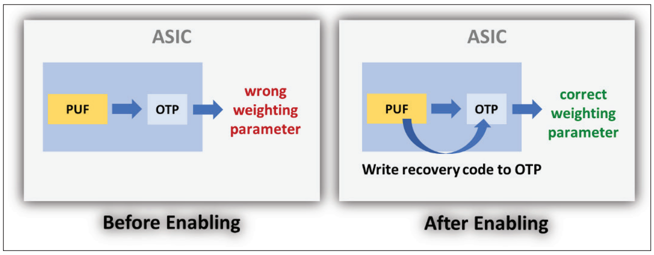
One of the key challenges for AIoT is the protection of AI assets. AI functions often need to detect, evaluate, and respond in real time. As a result, a critical security concern is the fact that internal databases and interfaces for AI are not suitable for encryption because such an operation would demand too much time and resources. However, big data and interface designs are all proprietary information that need to be securely protected. The data needed by AI systems is typically so large that it is usually stored in an external non-volatile memory (NVM), thereby exposing it to hacking risks that are increasing worldwide.

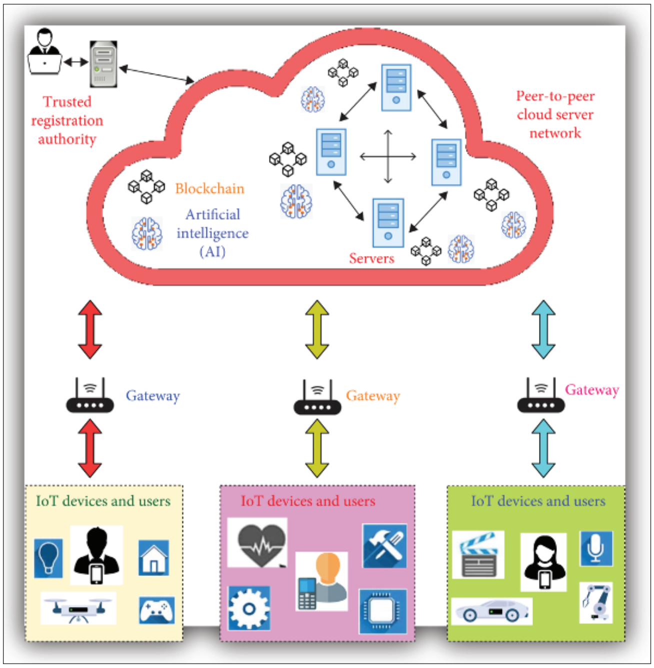
Meanwhile, in addition to the "internal" security issues of AIoT systems, the external challenges of AIoT security have also increased. Nearly two million cyberattacks in 2018 resulted in more than US$45 billion in losses worldwide as governments struggled with ransomware and other malicious incidents.

It is clear that while security concerns remain unresolved, the deployment of AIoT devices will increase attack vectors for intrusions. Therefore, PUF-based hardware security is the perfect solution for AIoT devices. With physical unclonable function (PUF), the existing trade-off of security for performance is eliminated.

PUF is a hardware security technology based on the physical unclonable variations occurring in the silicon manufacturing process. The underlying benefit of using a PUF in cryptography is its "uniqueness" and "unpredictability." With eMemory's PUF, a chip can generate truly random sequences that can be used in applications with high security requirements. This innovative technology can enable multi-layered security and resolve PUF-related concerns such as the additional costs of complicated error correction code (ECC). The random number extracted via PUF is so unique and unclonable that it can be used as a silicon "fingerprint" for a wide range of security purposes, including encryption, identification, authentication, and security key generation.

The dimension of attacks on AIoT include "data and firmware attacks," "transmission attacks," and "data integrity attacks." We understand that complex encryption and decryption are impractical for the protection of AI assets. PUF has become a relatively simple and fast solution for security. Below is an application scenario that could help you have a clearer picture of how PUF solves AIoT security concerns.


ASIC
PUF
OTP
wrong weighting parameter
Before Enabling
ASIC
PUF
OTP
correct weighting parameter
Write recovery code to OTP
After Enabling



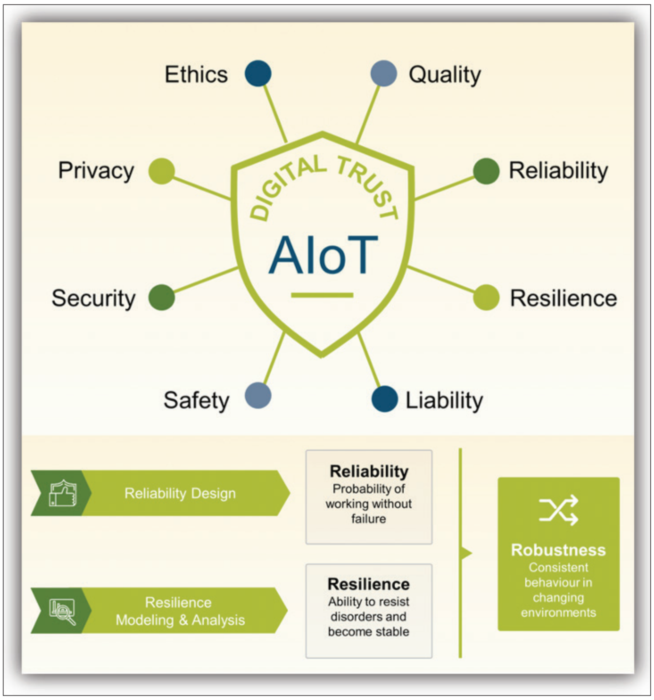
Architecture of blockchain-envisioned secure authentications framework for AIoT.

Trustworthiness

Trustworthiness is an overarching paradigm with a multitude of nuances and distinct aspects, having different connotations for different sets of stakeholders, use cases, and applications. A working definition of trustworthiness is the degree to which a user or other stakeholder has confidence that a product or system will behave as intended. This definition can be applied across the broad range of systems, technologies, and application domains. Characteristics of trustworthiness include reliability, availability, resilience, security, privacy, safety, accountability, transparency, integrity, authenticity, quality, usability, and accuracy. Trustworthiness is a foundational concern in the AI paradigm.

Digital trust (or trust in digital solutions) is a complex topic. When do users deem a digital product truly trustworthy? What if a physical product component is added, as in smart, connected products? While security is certainly a key enabler of digital trust, there are many other aspects that are important, including ethical considerations, data privacy, quality, and robustness (including reliability and resilience). Since AIoT-enabled products can have a direct physical impact on the well being of people, safety also plays an important role.

Safety is traditionally closely associated with verification and validation. The same holds true for robustness (reliability and resilience). We first need to understand the AI and IoT-specific challenges from a security point of view.


Ethics
Quality
Privacy
Reliability
DIGITAL TRUST
AIoT
Security
Resilience
Safety
Liability
Reliability Design
Resilience Modeling & Analysis
Reliability
Probability of working without failure
Resilience
Ability to resist disorders and become stable
Robustness
Consistent behaviour in changing environments

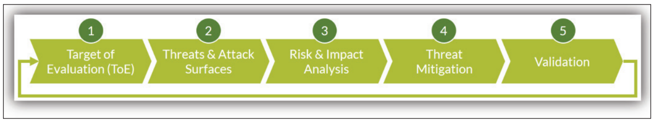
There are many potential ways to intentionally attack an AI-based system. A recent report from the Belfer Center describes two main classes of AI attacks: input attacks and poisoning attacks.

Input attacks: These kinds of attacks are possible because an AI model never covers 100 percent of all possible inputs. Instead, statistical assumptions are made, and mathematical functions are developed to allow creation of an abstract model of the real world derived from the training data. So-called adversarial attacks try to exploit this by manipulating input data in a way that confuses the AI model. For example, a small sticker added to a stop sign can confuse an autonomous vehicle and make it think that it is actually seeing a green light.

Poisoning attacks: This type of attack aims to corrupt the model itself, typically during the training process. For example, malicious training data could be inserted to install some kind of backdoor in the model. This could, for example, be used to bypass a building security system or confuse a military drone.

Security planning for AIoT must first determine the general approach. Next, threat modeling will provide insights into key threats and mitigation strategies. Finally, the security architecture and setup must be determined. Of course, this is an iterative approach, which requires continuous evaluation and refinement.

Threat modeling is a widely established approach for identifying and predicting security threats (using the attacker's point of view) and protecting IT assets by building a defense strategy that prepares the appropriate mitigation strategies. Threat models provide a comprehensive view of an organization's full attack surface and help to make decisions on how to prioritize security-related investments.



Securing an AIoT system is not a single task, and the results of the threat modeling exercise are likely to show attack scenarios of very different kinds. Some of these scenarios will have to be addressed during the phases of the DevSecOps cycle (e.g., during development and testing). However, some basic security measures can usually already be established as part of the system architecture and setup, including:

- Basic security measures, such as firewalls and anti-virus software
- Installation of network traffic monitors and port scanners
- Hardware-related security architecture measures, such as a trusted platform module (TPM), for extremely sensitive systems

These types of security-related architecture decisions should be made in close alignment with the product architecture team, early in the architecture design.

Minimum Viable Security

The key challenge with security planning and implementation is to find the right approach and the right level of required resource investments. If too little attention (and percent of project resources and budget) is given to security, there is a good chance that this will result in a disaster — fast. However, if the entire project is dominated by security, this can also be a problem. This relates to the resources allocated to different areas, but also to the danger of over-engineering the security solutions (and in the process making it too difficult to deliver the required features and usability). Figuring out the minimum viable security is something that must be done between product management and security experts. Also, it is important that this is seen as an ongoing effort, constantly reacting to new threats and supporting the system architecture as it evolves.

Trust Policy Management for AIoT

In addition to security-related activities, an AIoT product team should also consider taking a proactive approach toward broader trust policies. These trust policies can include topics such as:

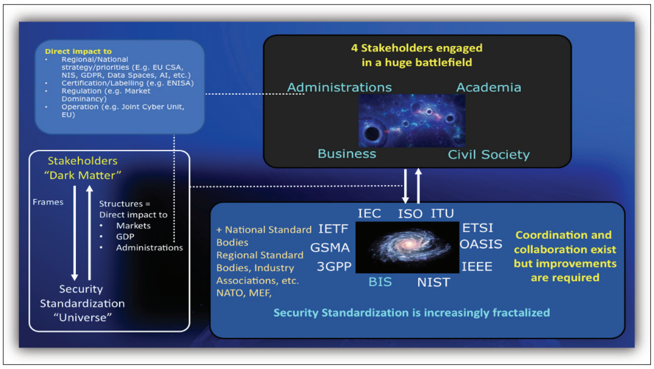
- Data sharing policies (e.g., sharing of IoT data with other stakeholders)
- Transparency policies (e.g., making data sharing policies transparent to end users)
- Ethics-related policies (e.g., for AI-based decisions)

Taking a holistic view of AIoT trust policies and establishing central trust policy management can significantly contribute to creating trust between all stakeholders involved.

The Standardization Conundrum

> "The beauty of standards is that there are so many to choose from!" — Andrew S. Tanenbaum, 1990.

In an ideal world, we would have exactly one standard for each task or interface. However, in reality, there are often overlapping or rivalling standards, driven by different vendor "camps," in case of cyber security, and standards by different global, regional, and national standards development orgranizations (SDOs). So, what can a designer or developer do? Support all standards? Too expensive. Wait for one standard to replace all others? May not happen. Implement a software abstraction layer that permits certain interfaces/standards to be replaced? Good, if possible. Choose one standard and accept incompatibility with all others? Bad, but sometimes the only choice.


Direct impact to
Regional/National strategy/priorities (E.g. EU CSA, NIS, GDPR, Data Spaces, AI, etc.)
Certification/Labelling (e.g. ENISA)
Regulation (e.g. Market Dominancy)
Operation (e.g. Joint Cyber Unit, EU)
4 Stakeholders engaged in a huge battlefield
Administrations
Academia
Business
Civil Society
Stakeholders "Dark Matter"
Frames
Structures = Direct impact to
Markets
GDP
Administrations
Security Standardization "Universe"
IEC
ISO
ITU
+ National Standard Bodies
Regional Standard Bodies, Industry Associations, etc. NATO, MEF,
IETF
GSMA
3GPP
ETSI
OASIS
IEEE
BIS
NIST
Coordination and collaboration exist but improvements are required
Security Standardization is increasingly fractalized

Global standardization ecosystem for cyber security.

The irony is that standards and even SDOs are not at the forefront of solution designers', developers', providers', deployers', or users' minds. There are misconceptions on what standards are for, and the case for use of standards has not been made. Most researchers, design engineers, and even startups argue that standards block innovation. In fact, standardization brings innovation and spreads knowledge. Standardization helps define the contours of structured innovation, first because it provides structured methods and reliable data that save time in the innovation process, and second because it makes it easier to disseminate ground-breaking ideas and knowledge about leading edge techniques. Liberalization and markets have a lot of great virtues, but they cannot create their own conditions of existence: they must be designed!

The AIoT value chain is perhaps the most diverse and complicated value chain of any industry or consortium that exists in the world. In fact, the gold rush to AIoT and IoT is so pervasive that if you combine much of the value chains of most industry trade associations, standards bodies, and the ecosystem partners of trade associations and standards bodies, and then add in the different technology providers feeding those industries, you get close to understanding the scope of the task. In this absolutely heterogeneous scenario, coming up with common harmonized standards is a major hurdle.

Most of the standards activity in the domain to date have been on the development of communication security, device security, and IT cyber security standards that address individual limited security concerns of different stakeholders. In the case of AIoT comprehensive security, it is unlikely to be which standard but which standards, since most architectures do not pick one standard but have a layered approach capable of using multiple standards in the portfolio.

Standards for AI are still in the nascent stage of development, and the global SDOs and stakeholders are still trying to unravel the diverse trustworthiness aspects and their respective validation and verification approaches, as they are highly context-deprendent. Hence, it would be prudent to assume that in any AIoT system security and trustworthiness assurance, compliance and/or certification would be a very nuanced issue and may need to be handled with utmost caution.

The multiplicity of technologies and their convergence in many new and emerging markets, however, particularly those involving large-scale infrastructure, demand a top-down approach to standardization, starting at the system or system architecture rather than at the product level. Therefore, the systems work will define and strengthen the systems approach throughout the technical community to ensure that highly complex market sectors can be properly addressed and supported. It promotes increased cooperation with many other SDOs and relevant non-standards bodies needed on an international level.

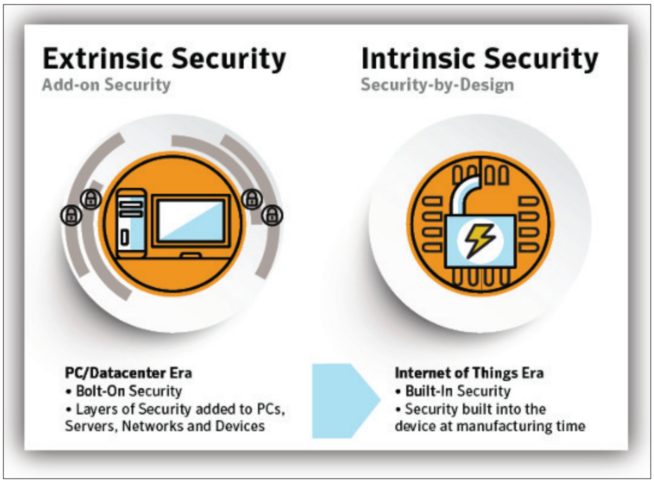
Hence, somebody has to orchestrate the symphony of standards and develop system standards covering the diverse security concerns of all the stakeholders comprehensively.

It is necessary to build a comprehensive inventory of security and trustworthiness concerns in different aspects of the AIoT paradigm followed by mapping them with corresponding technologies, processes, strategies, and standards, and developing a corresponding compliance testing framework and strategy. We need to study and analyze the diverse use cases, applications, and corresponding stakeholders and their respective requirements to understand their respective characteristics and concerns. We need to develop a granular architecture followed by developing a cyber security architecture mapping all the security, privacy, safety, and resilience characteristics with the granular architecture of any AIoT solution.

However, first of all, the diverse and complex AIoT paradigm needs to be mapped to a structured reference architecture and its relevant viewpoints to help map the whole spectrum of security standards to different blocks, layers, aspects, use cases, applications, security concerns, and stakeholders and their diverse concerns to understand the GAPS in standards and developing new systems standards and product-/domain-specific standards. This shall need to be followed by developing a comprehensive compliance testing framework and ecosystem of test labs, supporting and enabling services.

Without this comprehensive and granular exercise, the AIoT products, systems. and solutions shall NOT be considered secure and trustworthy.

Security Philosophy



Conclusion

Cyber Immunity and Cyber Resilience

- The pandemic-induced digital transformation has increased exposure to cyber threats as we cross the digital fault line due to remote working and escalated online presence. To counter this, an intuitive and adaptive cyber posture defined by zero latency networks and quantum leaps will be needed across industries. These developments, while great for humanity, will challenge privilege and privacy, and defend every citizen.
- The speed of processing of AI systems is currently seen as providing protection for infrastructures and networks

that human operators may not be able to match, especially as cyber-attackers are employing increasingly sophisticated methodologies. AI can potentially respond to a cyberattack scenario far more quickly than a human decision maker.

- Cyber immunity at every layer will create networks that are inherently secure and self-learning. AI-induced digital intuition is one of the pillars of cyber-security strategy that will allow intelligent adaption. The ability of AI systems to out-innovate malicious attacks by mimicking various aspects of human immunity will be the line of defence to attain cyber resilience based on both supervised and unsupervised ML.
- These systems will be designed to make the right decisions with the context-based data, preempt attacks on the basis of initial indicators of compromise or attack, and take intuitive remediated measures, allowing any digital infrastructure and organization to be more Resilient.

Biography

N. Kishor Narang (kishor@narnix.com) is a technology consultant, mentor, and design architect in electrical, electronics, and ICT with over 40 years of professional experience in education, research, design, and consulting. He has over 30 years of hardcore research, design, and development experience in fields as diverse as industrial engineering, power and energy engineering, IT, telecommunications, medical devices, and environmental engineering. Professionally, he is an electronics design engineer practicing design and development across a wide spectrum of products, systems, and solutions through his own independent design house, NARNIX, since 1981. For the last 10 years, he has been deeply involved in standardization in the electrical, electronics, communications, and information technology domains with a focus on identifying gaps in standards to bring harmonization through standardized interfaces to ensure end-to-end Interoperability. He has been leading national standardization initiatives at BIS, the Indian national standards development organization, in smart cities, smart manufacturing, smart energy, and active assisted living as the Chairman of the Smart Infrastructure Sectional Committee LITD 28, along with contributing to multiple other SDOs and initiatives. Globally, he is Vice Chair-Strategy and Project Leader of two international standards in IEC SyC Smart Cities, a Co-Editor of the ISO/IEC JTC1/WG 11 Four Standards, and a member of the Steering Committee of OCEANIS, beyond proactive contributions in many committees in global SDOs.

FOOTNOTES

[1] Mark Weiser, “The Computer for the 21st Century,” *Scientific American*, Sept. 1991.