IoT

How Technology is Helping Overcome Legal and Ethical Challenges

Solution Whitepaper

Table of Content

SECTION 1 – INTRODUCTION

Internet of Things (IoT), core to the Fourth Industrial Revolution, is growing rapidly. It is now a part of our daily lives and activities everywhere: in transit, at home, or office.

Recognizing its effectiveness, fungibility, and reliability, industries and companies across geographies are integrating IoT in operations to optimize resources, track performances, and maximize outputs.

Implementation of IoT comes with challenges related to:

1. Privacy and cybersecurity
2. Building a business environment that can support IoT
3. Inadequate governance structures
4. Lack of interoperability

Salient points covered in this report

We have tried to identify:

A. Areas that need monitoring;

B. Gaps in laws and ethical grounds that organizations need to be aware of; and

C. Companies with expertise in cybersecurity solutions and innovative startups that are designing ground-breaking software and solutions for IoT security.

Who should read this report?

A. Organizations that apply IoT in various functions but face security issues

B. Technologists and designers of devices or networks looking to improve their understanding of how to enhance the cybersecurity and privacy of their products/platforms

C. Policymakers, industry lobbyists, and legal consultants working on coming up with tighter laws related to cybersecurity

SECTION 2 – ETHICAL ISSUES AND CHALLENGES

Today, IoT has permeated every aspect of our lives, from personal to professional. We are continuously tracked and heard, whether we like it or not. Due to the extensive penetration of smartphones, home assistants, and other devices, companies have access to a vast pool of data that could be analyzed and used. However, the extent to which data can be gathered, recorded, and used presents an ethical as well as legal dilemma:

- Use of IoT in almost every device poses a risk to the privacy of individuals and companies.
- Security of data is threatened. Hacking of confidential documents, financial details, legal papers, and client data on company servers means major losses.
- Data usability and data user experience are affected.
- Organizations stand to lose trust if safety of data is compromised.

Despite the laws and regulations, monitoring is far from desired, leaving gaps in data privacy and security.

Critical safety issues are:

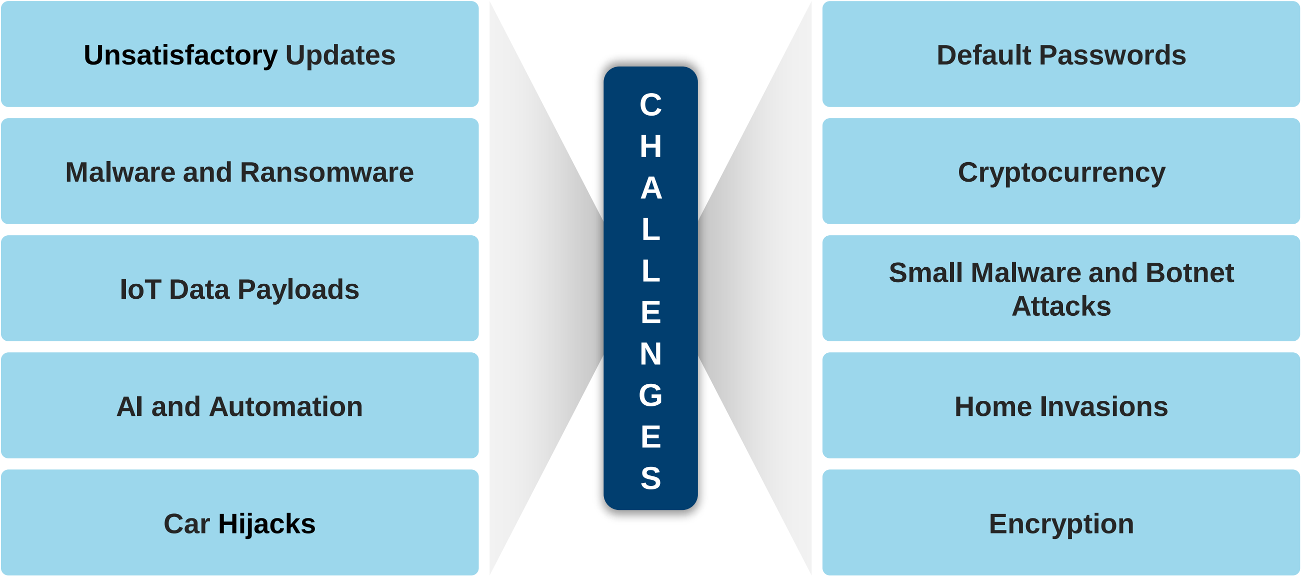
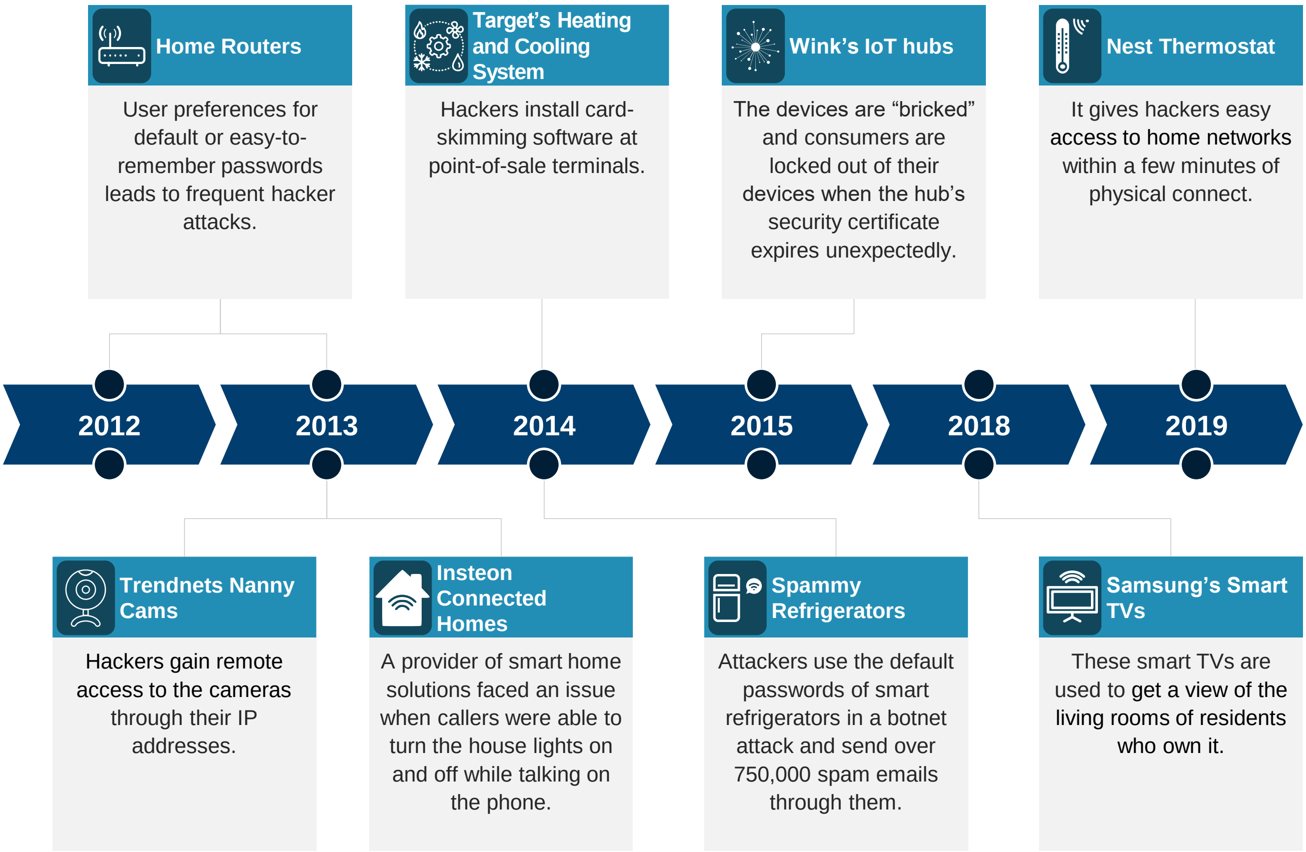


Figure 1: Key Challenges in Implementation of Cybersecurity Measures

SECTION 3 – SECURITY BREACHES



Home Routers

User preferences for default or easy-to-remember passwords leads to frequent hacker attacks.

Target's Heating and Cooling System

Hackers install card-skimming software at point-of-sale terminals.

Wink's IoT hubs

The devices are “bricked” and consumers are locked out of their devices when the hub's security certificate expires unexpectedly.

Nest Thermostat

It gives hackers easy access to home networks within a few minutes of physical connect.

2012 2013 2014 2015 2018 2019

Trendnets Nanny Cams

Hackers gain remote access to the cameras through their IP addresses.

Insteon Connected Homes

A provider of smart home solutions faced an issue when callers were able to turn the house lights on and off while talking on the phone.

Spammy Refrigerators

Attackers use the default passwords of smart refrigerators in a botnet attack and send over 750,000 spam emails through them.

Samsung's Smart TVs

These smart TVs are used to get a view of the living rooms of residents who own it.

Figure 2: Instances of IoT Security Breaches

Cybersecurity should be the topmost priority while creating and installing IoT devices to ensure protection from invaders.

There is a strong need to revamp laws in the domain and question the efficacy of existing rules and regulations. Are these adequate to address existing issues and stringent enough to safeguard people's interests? It also raises questions about the responsibility of the government - is it doing enough to ensure that the country is not just connected but safely connected?

SECTION 4 – ROLE OF GOVERNMENT

Governments of various countries are collaborating to come up with a corpus of laws for regulating implementation of IoT and ensuring security against threats to IoT applications. These regulations would be applicable to connected devices, the networks they reside on, and the cybersecurity and data associated with these devices.

For the laws to be effective, ethical practices need to be determined, as what is unethical may not necessarily be illegal. A set of guidelines, which is further protected by contractual agreements, must be drafted.

With regard to privacy, the European Union General Data Protection Regulations (EU GDPR 2016, etc.) and federal laws in the US form the basis for principles to govern the processing of personal information. The principle of 'Privacy by Design' has been added to EU GDPR 2016 Figure 3 shows the different aspects that an IoT privacy framework should include, as per UNIFY-IoT PROJECT: Policy Recommendation of the Uptake of IoT in the European Region.

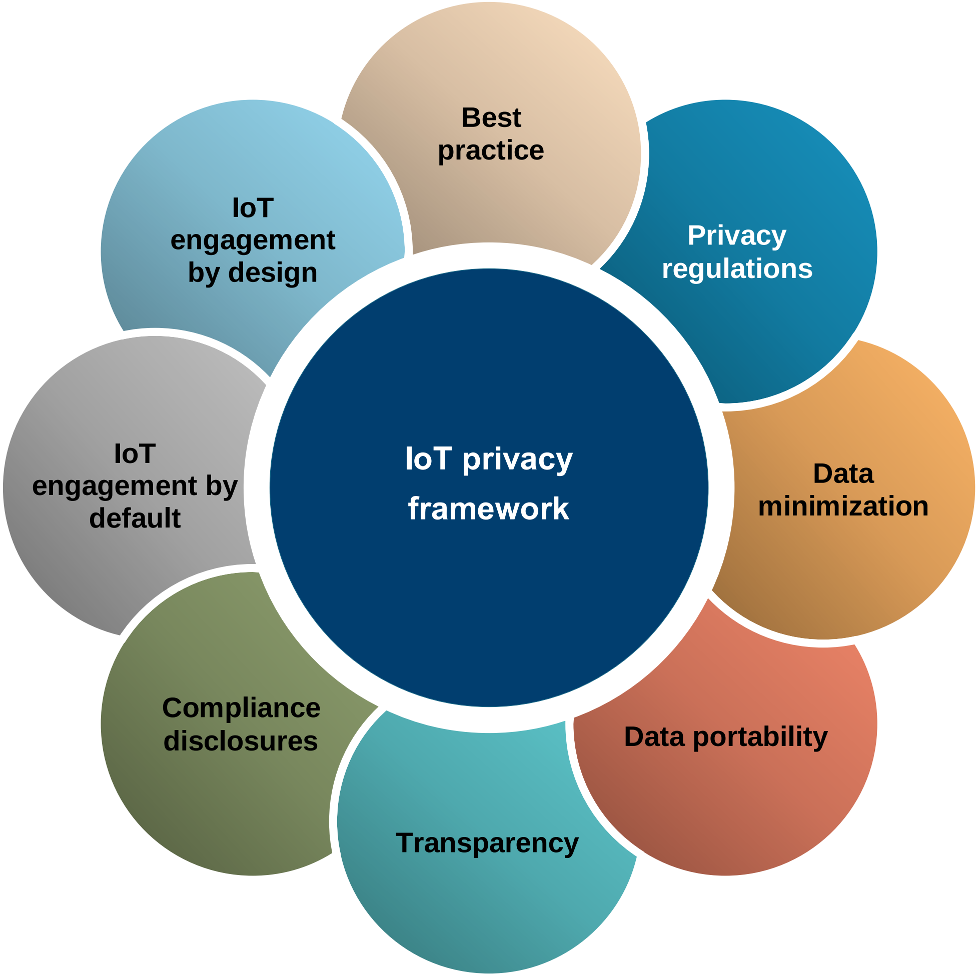


Figure 3: Ideal IoT Privacy Framework

Moreover, “trust” can have different interpretations. Figure 4 depicts a trust framework, which includes general principles for dealing with critical issues:

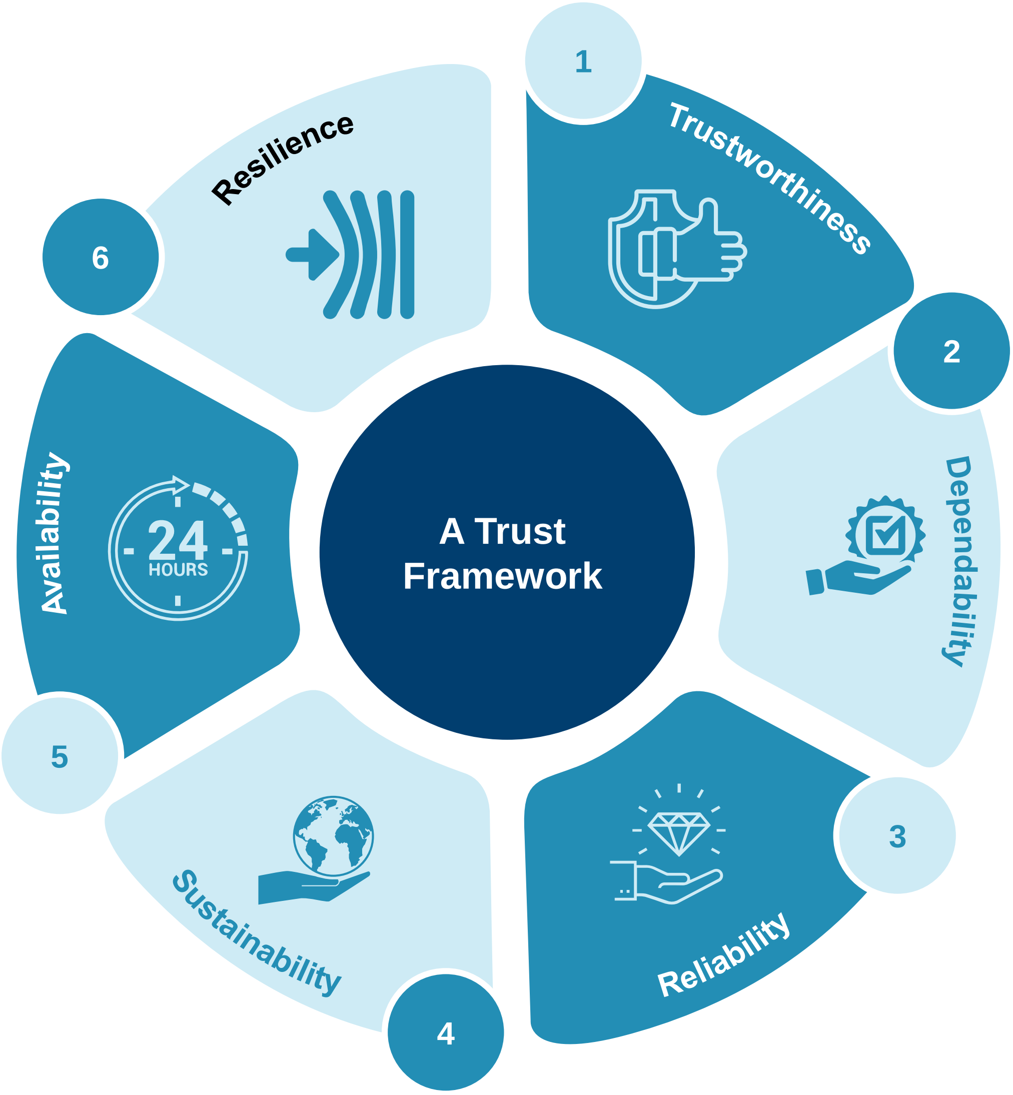
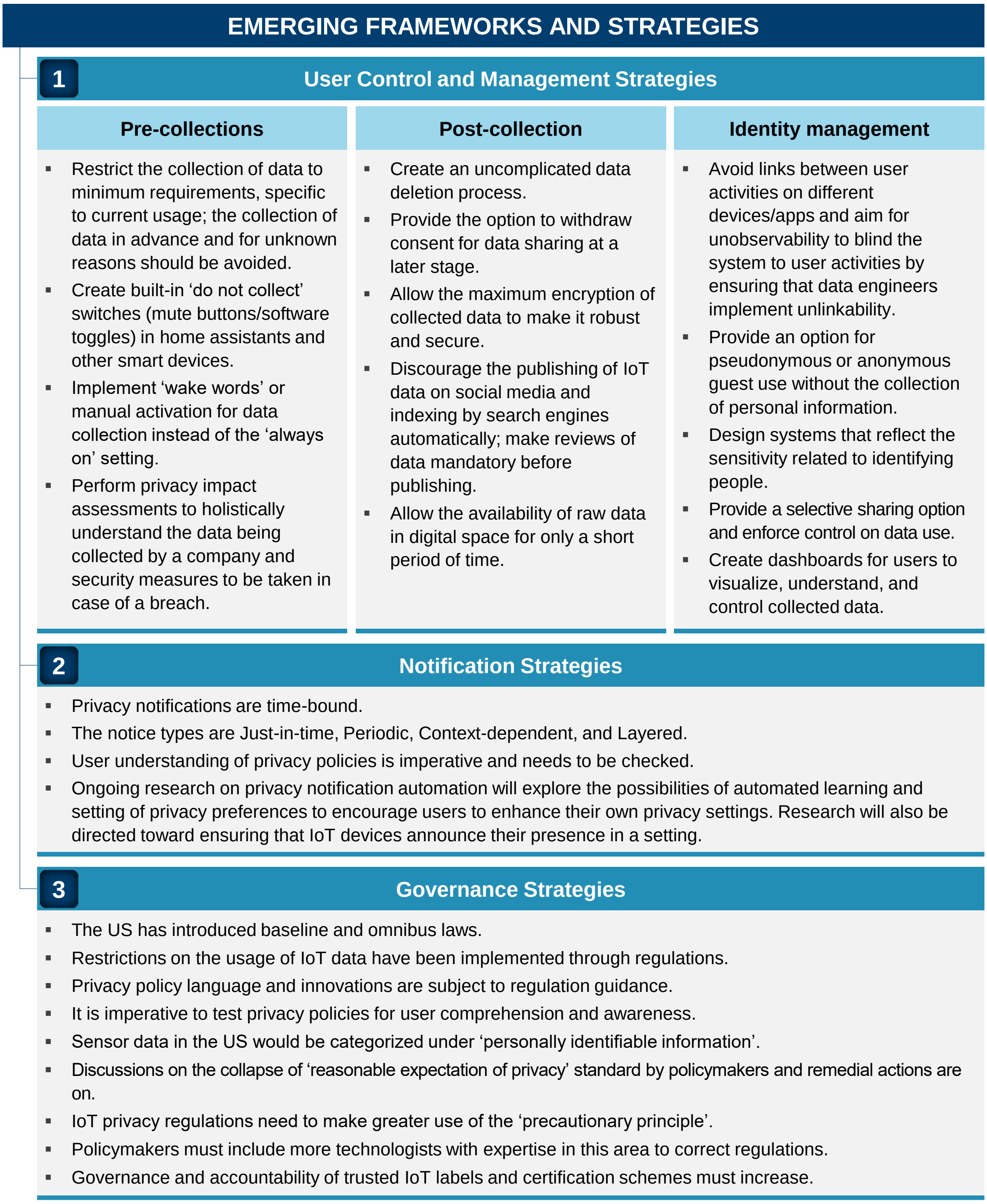


Figure 4: Trust Framework

The guidelines for IoT security would need to be drafted around the framework mentioned above and be more specific and flexible to permit the incorporation of new innovations in this space. To supplement the efforts of governments and associations (working for internet safety) in tackling cybersecurity breaches, clearly defined framework and strategies for data collection need to be followed.

SECTION 5 – EMERGING FRAMEWORKS AND STRATEGIES

Framework and strategies for IoT practices should be based on user control and management, notification, and finally governance. The user control and management strategy is employed across all three stages: pre-collection, post-collection, and identity management, as shown in Figure 5.



EMERGING FRAMEWORKS AND STRATEGIES

1 User Control and Management Strategies

Pre-collections

- Restrict the collection of data to minimum requirements, specific to current usage; the collection of data in advance and for unknown reasons should be avoided.
- Create built-in 'do not collect' switches (mute buttons/software toggles) in home assistants and other smart devices.
- Implement 'wake words' or manual activation for data collection instead of the 'always on' setting.
- Perform privacy impact assessments to holistically understand the data being collected by a company and security measures to be taken in case of a breach.

Post-collection

- Create an uncomplicated data deletion process.
- Provide the option to withdraw consent for data sharing at a later stage.
- Allow the maximum encryption of collected data to make it robust and secure.
- Discourage the publishing of IoT data on social media and indexing by search engines automatically; make reviews of data mandatory before publishing.
- Allow the availability of raw data in digital space for only a short period of time.

Identity management

- Avoid links between user activities on different devices/apps and aim for unobservability to blind the system to user activities by ensuring that data engineers implement unlinkability.
- Provide an option for pseudonymous or anonymous guest use without the collection of personal information.
- Design systems that reflect the sensitivity related to identifying people.
- Provide a selective sharing option and enforce control on data use.
- Create dashboards for users to visualize, understand, and control collected data.

2 Notification Strategies

- Privacy notifications are time-bound.
- The notice types are Just-in-time, Periodic, Context-dependent, and Layered.
- User understanding of privacy policies is imperative and needs to be checked.
- Ongoing research on privacy notification automation will explore the possibilities of automated learning and setting of privacy preferences to encourage users to enhance their own privacy settings. Research will also be directed toward ensuring that IoT devices announce their presence in a setting.

3 Governance Strategies

- The US has introduced baseline and omnibus laws.
- Restrictions on the usage of IoT data have been implemented through regulations.
- Privacy policy language and innovations are subject to regulation guidance.
- It is imperative to test privacy policies for user comprehension and awareness.
- Sensor data in the US would be categorized under 'personally identifiable information'.
- Discussions on the collapse of 'reasonable expectation of privacy' standard by policymakers and remedial actions are on.
- IoT privacy regulations need to make greater use of the 'precautionary principle'.
- Policymakers must include more technologists with expertise in this area to correct regulations.
- Governance and accountability of trusted IoT labels and certification schemes must increase.

Figure 5: Emerging Frameworks and Strategies

Precautions taken by companies while gathering information and storing do not guarantee security. Cybersecurity needs to be more ingrained into the system to protect against any kind of damage or theft.

SECTION 6 – A POSSIBLE WAY FORWARD: HIGHLY SECURE DEVICES

Ensuring devices connected to the internet are highly secure would probably go a long way in plugging data leaks and eliminating the risk of data piracy. This would require considerable innovation and planning. Microsoft has invented highly sophisticated cybersecurity methods to track the performance and safety of devices. Some properties of highly secure devices are:

1. **Hardware-based root of trust:** Hardware constitutes the core of any device. Two features make hardware naturally resistant or less vulnerable to any attack. First, it usually has one sole purpose and, therefore, cannot be used by hackers for any other purpose. Second, hardware is engineered to check for and defend against attacks. Thus, hardware can provide the foundation to build a robust security architecture.
2. **Compact trusted computing base (TCB):** All cybersecurity implementations for software and hardware are placed in the TCB of a device. This part, therefore, needs to be so compact that hackers, even if they can, are able to access only a very small section of it, rendering minimal damage.
3. **In-depth defense:** A completely secure device has multiple layers of defense. While it may be easy for hackers to circumvent one or two layers of security, multiple layers with different defense mechanisms may confuse them.
4. **Compartmentalization:** Dividing software into smaller compartments acts as a hedge against theft—even if there is a breach in one section, not necessarily all others would be compromised. Moreover, compartmentalization creates another layer of security, further safeguarding the device. However, this system is employed in very few devices.
5. **Certificate-based authentication:** To strengthen security, it is recommended that certificates, instead of passwords, be used to check identities for authentication when communicating with other devices and cloud. A certificate is an identity code that needs a private and public key. It cannot be stolen, forged, or impersonated, and thereby provides a solid wall of defense.
6. **Renewable security:** For hackers, destroying security walls is an everyday job. A device fortified with a renewable security element can revive and rebuild its security after an initial attack. The system is designed to remedy the breaches made and build a new wall of defense. Rollback protection eliminates the vulnerability of a device.
7. **Failure reporting:** Failure reports are automatically generated and sent to the user in case of a failed attack, for example, an unsuccessful attempt by a hacker to enter the device. These reports help in tracking attacks and planning defense thereafter. Without these reports, it would be extremely difficult to differentiate between defective programming and an attack.

SECTION 7 – END-TO-END SECURITY

With the advent of IoT, a reliable, sophisticated and flexible cybersecurity system has become a necessity. Some of the firms that provide security solutions are Microsoft, Azeti Networks AG, Intel, Sypris, Zingbox, and Shodan.

To illustrate the efficacy of such systems, we have considered Microsoft.

Microsoft discerned the importance of a blanket security system that covers the hardware, software, and cloud in a device. With this objective in mind, and after in-depth research in collaboration with various device manufacturers to understand the requirement in totality, it introduced Azure Sphere.

Azure Sphere is based on the seven essential properties of a highly secure device discussed in Section 7. Its three main components are:

Azure Sphere Microcontroller (MCU), i.e., Hardware Security: The basic principle on which microcontrollers work is to facilitate the operations and tasks of computers and appliances. Microsoft has also developed MediaTek MT3620, an Azure Sphere chip, which has built-in Microsoft security technology and connectivity.

Azure Sphere MCU can be used to enable secure connections for older IoT devices as well. In cases where Azure Sphere MCUs serve as 'guardian modules' for existing IoT devices, they can permit older, disconnected IoT equipment to be reconnected, thereby adding value.

Azure Sphere Operating System (OS), i.e., Software Security: This is an extremely secure software based on open source Linux OS. The Linux-based OS combines the Windows security technology and invention with a custom Linux kernel to create a secure software environment. The OS facilitates a completely safe connection with cloud. It has multiple layers of defense for the firmware and application code.

Azure Sphere Security Service, i.e., Cloud Security: This service entails providing cloud security to protect the Azure Sphere device. As IoT integrates with cloud, it is an essential service. It uses 'certificate-based authentication' to secure device-to-device communications. The services includes monitoring, detection, and reporting of cybersecurity threats.

Figure 6 depicts Microsoft's Azure Sphere.

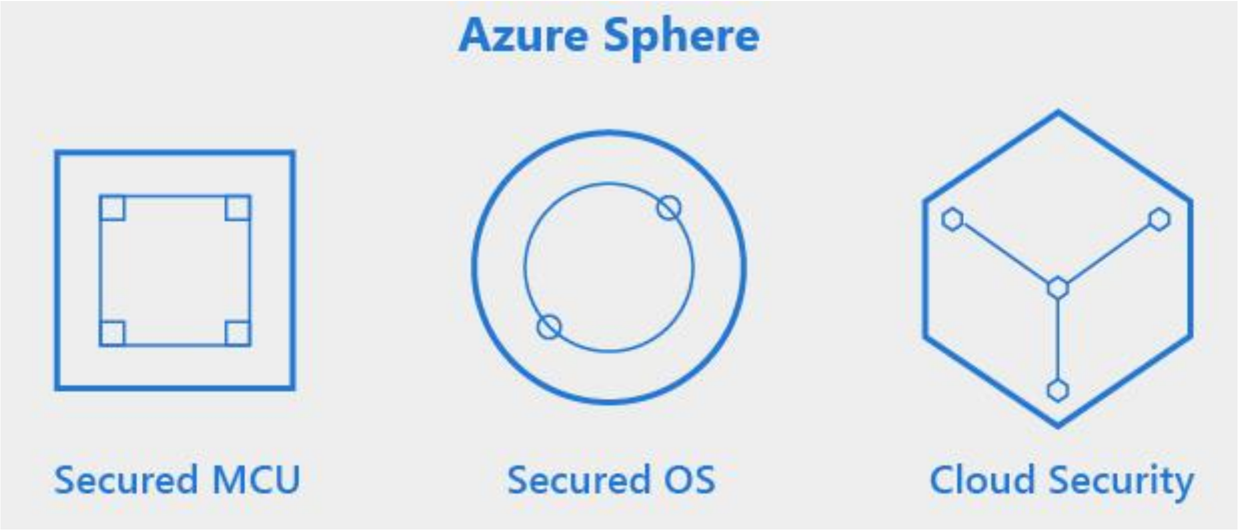


Figure 6: Azure Sphere

SECTION 8 – START-UPS IN THIS SPACE

Tapping the need to address cybersecurity challenges, several enterprises have mushroomed in this space.

1. **Bayshore Networks –** It mainly focuses on intrusion protection for IoT. Its industrial cyber protection software facilitates constant per-asset intrusion prevention throughout the network.
2. **Claroty –** The company primarily focuses on cybersecurity of operational technology (OT) networks, which are increasingly vulnerable to persistent cyberattacks. Claroty's cybersecurity platforms are designed to identify and eliminate misconfigurations and insecure connections. The company claims its network can easily adapt to any environment.
3. **Crypto Quantique –** The company is focusing on quantum technology, which it believes will redefine the overall security architecture. The technology relies on quantum-driven secure chips to provide maximum security for each device.
4. **Karamba –** Focusing mainly on IoT in the automobile sector, the company provides technology to safeguard electronic control units in cars. Karamba believes this would stop high-profile car hijacks related to IoT devices.
5. **Ultimo Digital Technologies –** The company created a blockchain-enabled ecosystem with technology to trace and authenticate IoT data. The system helps track every step in a supply chain.
6. **Iotic –** The company introduced a concept, 'digital twins'. This security measure creates an intelligent digital twin of a connected IoT device, thereby allowing data interoperability and secure interactions.
7. **MagicCube –** The company's eponymous tech virtualizes the function of hardware security and creates a virtual vault that can practically reside in any IoT device, regardless of the manufacturer.
8. **Armis Security –** Armis's cybersecurity solution helps organizations detect risky behavior of connected devices in the network and eliminate them.
9. **PFP Cybersecurity –** The company offers 24X7 monitoring and remediation of all IoT devices and helps prevent hardware and firmware intrusion alongside configuration and data issues.
10. **Sepio Systems –** The company's software uses behavioral analytics and physical fingerprinting technology to detect and correctly respond to attempted breaches.
11. **Trillium Secure –** The company has designed a platform that protects vehicles from cyber threats, using trusted data, applications, and services.

SECTION 9 – CONCLUSION

Any technological or industrial revolution brings concerns regarding safety, job security, and economic growth in its wake. IoT is no different. As IoT security technology matures, threats are also becoming more sophisticated, with hackers finding new ways to attack IoT devices and protocols. This creates the need for updatable hardware and software for new IoT devices with a special focus on cybersecurity.

Tech-giants are building chip-to-cloud, end-to-end security management solutions specifically targeted at high-growth IoT markets, indicating a shift in focus to end-to-end security approach with embedded safety by design. This, along with the reliance on solution providers and system integrators with clear service level agreements (SLAs) for security and privacy, would hopefully pave the way for efficient IoT security systems from the perspective of organizations.

Governments and regulatory bodies are working together to implement secure, ethical, and legal IoT. Discussions on regulations and policies related to IoT security are rising in the European Union and the US. Furthermore, increasing standardization, specification, reference architectures, and formulation of best practice guidelines would support IoT security. Governments need to take similar steps in deploying robust regulatory and cybersecurity standards. Any non-compliance with regulations should be punishable.

Development in adjacent technology areas, such as edge computing, artificial intelligence for real-time security monitoring, and blockchain, facilitates the integration of these technologies for IoT security, thereby strengthening it.

Communication and awareness exercises to educate users about product-related risks are necessary to ensure safety.

Data collection should be minimal and restricted. Companies need to avoid unethical practices and have stringent policies in this regard that should be reviewed and updated regularly. They should understand from the consumer’s perspective what would be regarded as unethical or breach of privacy.

While issues related to cybersecurity and privacy of IoT devices are being addressed, there is still a long way to go. Until an efficient acceptable standard for IoT security and privacy is established, companies, governments, and consumers need to work collectively to mitigate threats. The primary concern should be to thwart attacks that can cause damage and create chaos in the political, military, economic and/or social spheres.

About Aranca

Founded in 2003, Aranca is a global research & advisory services firm working with clients worldwide across financial markets, industry sectors and technology domains. Aranca brings to play the strong combination of best data and best talent to empower decision makers with intelligence and insights, enabling them to reach better business decisions. Our multi-disciplinary expertise is designed to cater to clients of all sizes across a wide spectrum, from Fortune 500 companies and financial institutions to private equity and high potential startups. In the MENA region, Aranca works with some of the top family groups, private equity and investment management firms with strong focus on strategic corporate and financial advisory services.

Disclaimer

The information contained herein is believed to be obtained from the reliable sources and Aranca disclaims all warranties as to the accuracy, adequacy and completeness of such information.

Since Aranca is not a law firm, it (including its directors, employees and representatives) does not and cannot render legal services/advice to any individual or entity in any part of the world.

Authors

Neha Tapase

Assistant Manager

Technology Research & Advisory

Shreya Das

Content Manager

Publications

Aranca

Unit 201 & 301, Floor 2 & 3, B Wing, Supreme
Business Park, Hiranandani Gardens, Powai,
Mumbai – 400 076

+91 22 3937 9999

www.aranca.com | www.linkedin.com/company/aranca

aranca