IoT

Solution Whitepaper

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 3 – SECURITY BREACHES

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.

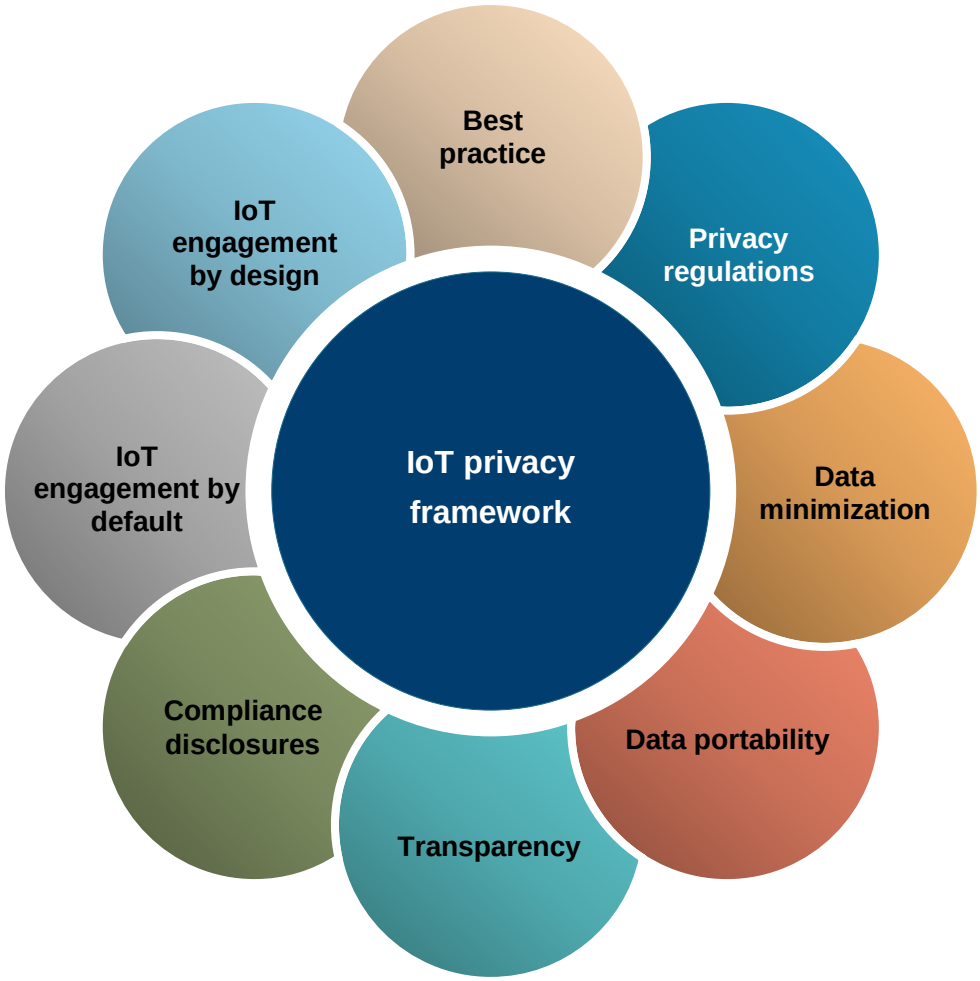

Figure 3: Ideal IoT Privacy Framework

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.

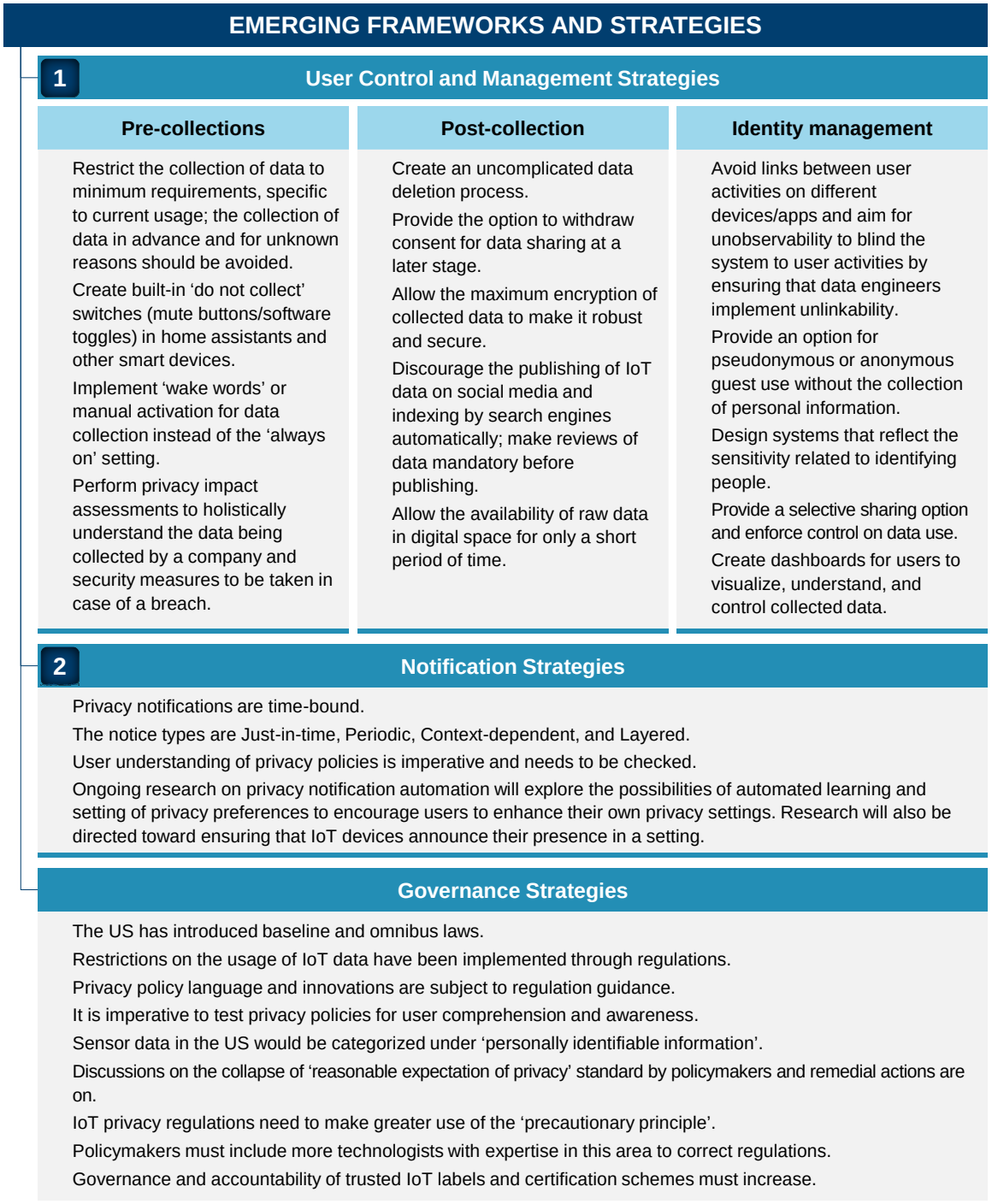

Figure 5: Emerging Frameworks and Strategies

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 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

About Aranca

Disclaimer

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