Addressing Security and Privacy Concerns to Realize IoT's Potential

Abstract

The Internet of Things (IoT) opens new possibilities for businesses to deliver incredible value to customers. However, the reliability, security, and privacy of IoT technologies are major concerns for users and businesses as the ultimate goal of IoT is to create secured and privacy-enabled smart services that consumers can trust.

Understanding the Growth of the Internet of Things

IoT provides several breakthrough functionalities to improve the quality of life and enables technological advances in critical areas. The applications span personalized healthcare, emergency response, traffic management, smart manufacturing, defense, home security, and smart energy distribution and utilization, among others.

Envisioning IoT-Enabled Smart Cities

According to TCS' Global Trend Study that surveyed over 800 enterprises across 13 industries, businesses are set to make huge investments in the IoT in the next 5 years—nearly 7% respondents planned to spend $500+ million in 2015.[1]

According to TCS' Global Trend Study that surveyed over 800 enterprises across 13 industries, businesses are set to make huge investments in the IoT in the next 5 years—nearly 7% respondents planned to spend $500+ million in 2015.[1]

The IoT can be leveraged to build a connected environment of interdependent systems, enhancing all aspects of urban life. This can be achieved by embedding IoT technology in all types of physical objects and artifacts ranging from clothes, home appliances, and automobiles to street lighting systems, transport systems, public utilities, and even the human body.

In a smart city, the IoT will be deployed to create a dynamic, digital fabric of interdependent systems, with instantaneous data gathering and near real-time analytics. Cities such as Barcelona in Spain, San Jose in the US, and Edinburgh in the UK are implementing smart services for their citizens, and India has plans to establish about 100 smart cities[5] in a decade.

IoT-Enabled Services Opening up a World of Possibilities

Functionally, the IoT sensors capture contextual data from a designated environment and send it to a centralized storage space that resides in the cloud. The contextual data is analyzed and processed in the cloud or at the edge to support various smart services. The monitoring and management of IoT devices, as well as their inter-communication, is performed remotely to optimize the smart services. This helps enterprises leverage the IoT to deliver superior services that make the various elements of our personal and public life truly smart.

However, there are notable privacy concerns around the user data gathered by IoT devices that need to be addressed early on.

Gartner's Hype Cycle for Emerging Technologies, 2015 shows that IoT is at the peak of inflated expectations[2] and on the cusp of multi-year, multifold growth. In 2020, 25 billion connected "things" will be in use.[3]

According to the British Standards Institution, a smart city is one that effectively integrates physical, spatial, digital, and human worlds to deliver a sustainable, prosperous, and inclusive future to its citizens.[4]

Strengthening Security and Privacy is the Key

Data security is a stumbling block in the intricate landscape of interconnected IoT systems.

Traditional security techniques are inadequate to manage the scale and complexity of IoT-enabled services. There are unique access control challenges and memory limitations that restrict the communication and processing capabilities of these devices to run complex encryption algorithms. These issues are further compounded by the distributed nature of the IoT device network, which is vital to create a system that provides context-aware services. In addition, non-trusted entities can physically or remotely intercept and manipulate data captured by IoT sensor nodes. Data transmission from sensors and gateway devices can be passively monitored in the absence of robust encryption, and malicious nodes can be embedded in wireless sensor networks to interfere with neighboring nodes.

Privacy is another pressing concern due to the possibility of misuse of Personally Identifiable Information (PII).

Smart healthcare systems, smart billing and payment systems, smart home security systems, smart fitting rooms in retail outlets, proximity marketing beacons, and smart vending machines all pose immediate and real potential security risks that need to be addressed.

A Holistic Security Solution

A comprehensive IoT security solution needs to be mapped to five key dimensions:

1. **Securing sensors:** Wireless sensors can be damaged, and memory and power limitations make them vulnerable to eavesdropping and radio jamming attacks. For outdoor smart services, periodic site surveys and regular physical checks are necessary to identify damaged sensors that need replacement.
2. **Safeguarding the network:** A network security policy for wireless connectivity needs to be defined, based on network security protocols such as Wi-Fi Protected Access 2. It outlines key security steps such as non-suggestive Service Set Identifier (SSID) for segmenting networks and ensuring client communication through designated access points. For wired networks, the security policy should include firewalls, intrusion prevention systems, and robust encryption mechanisms.

3. **Protecting data captured by sensors:** It is not feasible to encrypt contextual data using complex algorithms due to the limited computing power and energy storage capacity of IoT devices. Hence the data transfer from IoT devices needs to be secured to prevent data loss.
4. **Ensuring safe storage of data in the cloud:** The data collected by sensors is sent to the cloud for analytics, application-based processing and storage. It is essential to prevent data breaches and leaks in the cloud and to ensure effective data ownership.
5. **Gaining end-to-end control of devices, data, and networks:** To secure smart services and offerings, specifically in smart cities, it is imperative to track and control all interconnected devices, data, networks, and gateways that deliver these services. Attribute-based access control can be implemented to mitigate security risks.

Enhancing Privacy

Global regulations mandate the collection and processing of PII in a verifiable manner. Privacy can be broadly classified into four categories:

1. **Identity:** As IoT devices are owned by individuals and organizations, these can be used to identify their owners. Therefore, these devices and the data they generate should be marked as private.
2. **Location:** An IoT device's geo-position can be used to gather information about the owner's location. Such information needs to be concealed to prevent unscrupulous activities.
3. **Search query:** Search queries can reveal information about the person who initiated it by tracking the IP address of the source. Businesses can track queries and profile the owner based on his or her fondness for specific items. This data can then be used for targeted advertising without the individual's consent.
4. **Digital footprint:** As IoT-enabled devices are always online, they leave behind traceable data on the Internet. The devices should be secured through effective security protocols to avoid accumulation of digital footprints related to devices and their owners. Cookie invasion of IoT devices should also be prevented to ensure operational privacy.

Conclusion

FThe Internet of Things is a promising technological advancement that can offer several truly revolutionary benefits to society. However, it is only when businesses and city councils across the globe collaborate to build secure and reliable IoT systems, that the world will realize the full potential of this technology.

Structured and well-defined cyber security and privacy policies that protect citizens without stifling innovation will allow individuals and communities to reap the maximum advantages of IoT. It is then that IoT can really be leveraged to build a smarter world.

References

[1] Tata Consultancy Services, "Internet of Things: The Complete Reimaginative Force" (July 2015), http://sites.tcs.com/internet-of-things/#download-report

[2] Gartner, "Hype Cycle for Emerging Technologies, 2015" (July 2015), http://www.gartner.com/newsroom/id/3114217

[3] Gartner, "Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015" (November 2014), http://www.gartner.com/newsroom/id/2905717

[4] BSI, "PAS 181 Smart City Framework" (2014), http://www.bsigroup.com/en-GB/smart-cities/Smart-Cities-Standards-and-Publication/PAS-181-smart-cities-framework/

[5] Smart Cities Mission: Ministry of Urban Development: Government of India, "Smart City: Mission Statement & Guidelines" (June 2015), http://smartcities.gov.in/writereaddata/smartcityguidelines.pdf

About The Author

Abhik Chaudhuri

Abhik Chaudhuri is a Domain Consultant for cyber security, privacy and policy with TCS' Global Technology Practice. Chaudhuri has 14 years of IT experience and is a Chevening TCS Fellow in Cyber Security, Privacy and Policy.

About TCS' IT Infrastructure Services Unit

Leading organizations across industries work with TCS to realize their business transformation and innovation objectives by enhancing the availability, performance and agility of their IT infrastructure. Leveraging a combination of the cloud, new generation delivery models such as IaaS, PaaS, and SaaS, virtualization, and managed services, our offerings deliver the secure, flexible, and reliable IT infrastructure needed to power critical business applications, services and data.

TCS infrastructure offerings encompass data center services, end-user computing (EUC), mobility services, cloud services and transformational solutions, converged network services, managed security services, application management services, enterprise systems management, IT service desk, and IT service management. Backed by our Assess-Build-Manage-Transform framework, extensive partner ecosystem, tools and automation frameworks, and technology Centers of Excellence (CoEs), analytics-led approach, to understand the 'as-is' state, and arrive at the 'to-be' state. As a result, you seamlessly transition from traditional infrastructure management services towards new generation delivery.

Contact

VVisit TCS' IT Infrastructure Services unit page for more information

Email: itis.presales@tcs.com

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

TCS Design Services I M I 11 I 16