Analysis of Digital Trust in the Era of Internet of Things

유효문* · 이가배* · 이현창*· 연학박* · 진찬용* · 신성윤**

*원광대학교

**군산대학교

Analysis of Digital Trust in the Era of Internet of Things

Xiao-wen LIU · Jiapei Lee · Hyun-chang Lee* · Xiao-wen LIU · Chan-Yong Jin* · Seong-yoon Shin**

*Wonkwang University

**Kunsan University

E-mail : *20074696@wku.ac.kr *hclglory@gmail.com

요 약

In the digital business environment, digital trust has became a key element of business compete. With the Internet of Things(IoT) development, the success of businesses that participate in the world of connected devices depends on the level of digital trust consumers have in them. This paper introduced the definition and elements of digital trust , analyzed status of digital trust in IoT era, then puts forward the countermeasure of strengthening digital trust.

Key words: Digital trust, Internet of things(IoT), Electronic commerce

키워드

데이터분석, 사물인터넷, 트러스트

Ⅰ. 서 론

The explosive growth of the IoT has resulted in a highly connected digital ecosystem. The IoT empowers organizations to gather greater insights about their patients, customers, and users. Investment in the IoT is at an all-time high as organizations aim to deliver innovative new products and services that increase efficiency, improve customer experiences, and ultimately drive revenue.

In the IoT era, the digital world is upon us and everyone and everything is online. With so many connected devices coming online, it raises the question: can they be trusted with personal data? How do we build a digital world that we can trust? This paper will focus on these issues and done in-depth study.

Ⅱ. Definition and classes of digital trust

Trust is one of the fundamental constructs to any interaction in our society, it is the easiest to define and the hardest to implement. It relies on both transparency and making an effort to behave consistently. In the digital age trust has become essential, classical social trust concept has been stretched into to a concept that includes digital processing, Giustiniano and Bolici position trust in two different classes: social trust and technological trust as shown in Figure 1. Trust in the digital information age, called digital trust (or e-trust, or online trust) indicates a “positive and verifiable belief about the perceived reliability of a digital information source, leading to an intention to use”[1].

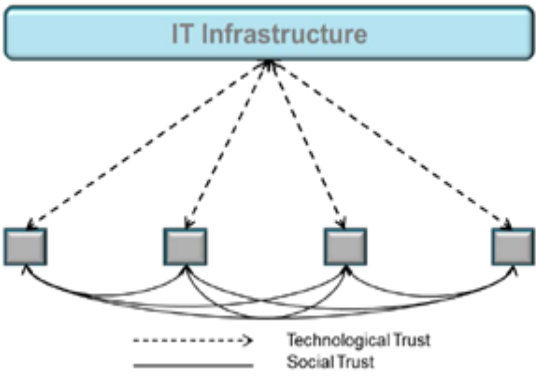

Fig 1. Trust in the digital information age

There are four key dimensions of digital trust presented by Accenture, It includes: Security Privacy,Data control, Accountability and Benefit/Value[2].Grandison and Sloman further to describe the digital trust in five digital trust classes, as shown in Table 1.

Table 1. Digital trust classes[3]

Digital trust classes	Description
Provision trust	Describes the trust in a service or resource provider when the trustor seeks protection from malicious or unreliable service providers.
Access trust	Describes trust in principals for the purpose of accessing resources owned by or under the responsibility of the trustor.
Delegation trust	Describes trust in an agent (the delegate) that acts and makes decision on behalf of the trustor.
Identity trust	Describes the belief that a trustee's identity is as claimed. Trust systems that derive identity trust are typically authentication schemes such as X.509 / PKI, PGP, and IBE3.
Context trust	Describes the extent to which the trustor believes that the necessary computer systems and institutions are in place to support an online activity and to provide a safety net in case something should go wrong.

Ⅲ. Survey and analysis of digital trust in IoT

According to a survey,83% people agree that digital trust is the cornerstone of the digital economy. As IoT matures, security and privacy risks will increase substantially. The success of businesses that participate in the world of connected devices depends on the level of digital trust consumers have in them. Digital trust is more than helping the IoT nodes to find a better trust to contact with, or reducing the uncertainty while they are interacting. In fact, trust is a hugely important factor. Consumers must have confidence that the organization is collecting, storing and using their digital information in a manner that benefits and protects them. As the IoT unleashes an exponential jump in the data businesses have on consumers, digital trust has been the gateway to monetizing its value.

Accenture's digital consumer survey addresses the current state of digital trust among consumers. The survey includes 23,000 respondents across 23 countries and demonstrates that the majority of consumers are concerned about the privacy and security of their digital personal data[4].

In the IoT era, globally only 45% of consumers have confidence in the security of their personal data. Digital trust in the security of personal data varies widely across the globe with developed markets expressing less digital trust overall Consumers in emerging markets, consisting mostly of the growth markets of Latin America and Asia, are more trusting, with 50 percent having confidence in the security of personal data compared to 41 percent of consumers in developed markets.Table 2 is the list of percentage of respondents in each country confident in the security of their personal data.

Table 2. Percentage of Respondents in Each Country Confident in the Security of their Personal Data[4]

Country /Area	Percentage	Country /Area	Percentage	Country /Area	Percentage
India	72%	Brazil	49%	Sweden	43%
Saudi Arabia	55%	South Africa	47%	France	38%
UAE	54%	Turkey	47%	Czech Republic	36%
UK	54%	Canada	45%	Korea	33%
Mexico	53%	China	45%	Germany	29%
Indonesia	51%	US	45%	Netherlands	27%
Spain	51%	Russia	44%	Japan	26%
Australia	49%	Italy	43%		

Digital trust also varies by age and gender. Only about one in three consumers aged 45 and older are confident in the security of personal information on the Internet. Furthermore, female consumers are significantly less confident than males overall in the security

of their personal information.

In Accenture's research, they also found that technology companies have the opportunity to build greater trust in aggregate as well as with specific target segments. Percentage of Respondents in India, U.K. and U.S. Identifying Each Brand (Up to 3 Brands Allowed).Consumers trust their banks with their personal data more than any single technology brand. Among the technology companies we queried, Google is the technology brand trusted by the most consumers, led by strong trust in India.Amazon is the technology brand ranking second in trust among the brands we investigated. Brands trusted with personal data shown as Table3.

Table 3. Brands Trusted with Personal Data[5]

Country /Area	Percentage	Country /Area	Percentage	Country /Area	Percentage
Bank	51%	Amazon	24%	Samsung	14%
Broadband Internet provider	29%	Facebook	19%	Sony	7%
Mobile phone network provider	29%	Apple	16%	Wikipedia	5%
Google	28%	Microsoft	15%	Twitter	5%

While some business functions may be more closely involved in building digital trust, the entire organization is impacted. Communications, media and technology companies must understand the larger impacts of digital trust across all customers and products and undertake a ross-organization effort to establish the appropriate measures to ensure security, privacy and data control, value, and accountability.

Table 4. Digital Trust Impacts the Entire Business[6]

Agents of Action	Security	Privacy/ Data Control	Benefit/Value	Accountability
Management &Finance	SLR	SLR	SLR	PR
Sales &Marketing	SLR	SLR	PR	SLR
Product Development & Support	SLR	PR	PR	SLR
Legal &Regulatory	SLR	PR	SLR	PR
IT	PR	SLR	SLR	SLR

SLR:Primary responsibility PR :Some level of responsibility

Ⅳ. Establish the digital trust in IoT

The majority of consumers remain cautious about sharing their personal information online and, when they do, they trust established brands more than other companies .The time is now to close the gap in consumer confidence and gain their digital trust. It is simply a prerequisite for those wanting to leverage the IoT business and technology opportunities that are just over the horizon.Furthermore, once a company captures trust, it leads to a perpetual trust cycle: consumers trust the brand and provide more data; from the data the brand creates more services, which establishes more loyalty and leads to more trust, which leads to more sharing of data[6].

Firstly, nominate a chief security officer. Companies should consider having a security officer who would attend meetings where the highest-ranking leaders make major strategic decisions. The officer should have a more direct reporting relationship to the chief executive officer, providing recommendations for the company's strategic direction from a security and data privacy perspective. In most large companies, executive board members tend to have a direct role in either protecting or building shareholder value. This top security officer's responsibilities would encompass this as well.

Secondly, evaluate product and service security risks. Companies need to rethink how to design and build products and services to make them more secure. More security needs to be built into each high tech product when it is designed. Security should protect a high tech company's products while adhering to ecosystem security requirements in which that product will be used. This also means that greater scrutiny is required for understanding the capabilities and risks for all partners within the IoT ecosystem, making it critical to develop the appropriate processes for screening and evaluating partner companies.

Thirdly, use proactive product testing methods. Companies should perform proactive tests to prepare for breaches. Tests should anticipate what could go wrong and take steps to avoid them. Companies should do active penetration testing that tries to hack into their own products. The goal should be to find security vulnerabilities so they can be

preemptively fixed. Perhaps most importantly at the board and c-level, information security must be considered a business priority and security objectives should be aligned with business requirements. Given the increasing number of data breaches and growing accountability at the highest levels within an organization, the risks are greater than ever before.

At last, establish customer trust. The company that can build a reputation for providing valuable services while using consumers' personal data in trustworthy ways could have big advantages over competitors. Strong digital trust could help brands attract and retain customers, offer new products and services and position themselves well within the larger value chain of goods and services.

Ⅴ. conclusion

In this IoT world, every business is a digital business. Digital trust is the currency of today and will be central to defining the high performers of tomorrow. A breach of trust can quickly result in harmful business consequences such as consumer alienation, brand erosion and churn. Many leading communications, media and technology companies recognize the dual importance of building digital trust both as a company, and as an enabler of the overall digital economy, making it critical for all companies in these industries to act now or be left behind.

Once companies gain digital trust, they can leverage IoT business and technology opportunities. Most importantly, they can access more consumer data from those who trust them, use analytics to unlock more value from that data, deepen customer loyalty and offer more relevant, revenue generating services and applications.

Reference

[1] Giustiniano, L., Bolici, F. (2012). Organizational trust in a networked world: Analysis of the interplay between social factors and Information and Communication Technology. Journal of Information, Communication and Ethics in Society, 10(3), 187-202.

[2] The four keys to digital trust: Don't be left behind. https://www.accenture.com/us-en/insight-accenture-four-keys-digital-trust

[3]Jøsang, A., Ismail, R., Boyd, C. (2007). A survey of trust and reputation systems for online service provision. Decision support systems, 43(2), 618-644.

[4] The Four Keys to Digital Trust - Accenture. https://www.accenture.com/t20150709T093453__w__/us-en/_acnmedia/Accenture/Conversion-Assets/LandingPage/Documents/3/Accenture-3-LT-7-Four-Keys-Digital-Trust.pdf.

[5] Digital Trust in the IoT Era.https://www.accenture.com/us-en/~/media/Accenture/Conversion-Assets/LandingPage/Documents/3/Accenture-3-LT-3-Digital-Trust-IoT-Era.pdf.

[6] Building Digital Trust The confidence to take risks. https://www.pwc.com/sg/en/publications/assets/build_digital_trust_201312.pdf.