

## **A Study on Trust ICT Business Models: Based on Disruptive Innovation Theory**

Song Minzheong  
Hansei University, Gunpo, Korea

**Abstract:** The purpose of this study is to develop trust ICT business models, not only to allow people to maintain control and receive the information and social network service benefit but also to be connected safely with IoTs and physical networks. For this, it firstly defines trust and trust ICT and discusses the disruptive innovation model as theoretical background. With this backdrop, it formulates the analysis framework for developing business models by three types of asymmetries such as information and service, solution and control asymmetries. As the result, trust ICT business models are proposed and the related use cases with new market disruption are shown. To solve the problem of information asymmetries, ephemeral messaging application, reputation related services and ID management solutions are recommended. To solve the problem of solution asymmetries, e-mail data management, consumer IoT data management and IoT management for companies are recommended. Lastly, to solve the problem of control asymmetries, device and companion app, consumer cloud storage and cloud management for companies are recommended.

**Key words:** Trust, ICT, business model, disruptive innovation, recommended, information

---

### **INTRODUCTION**

This study is concerned about ‘trust information and communication technology (hereafter, trust ICT)’. It refers to the ICT which has trustworthiness. Many firms manage high volumes of security incidents, breaches, malware and hackers. Early security offerings tended to focus on the network (e.g., WAN and Internet service security) and such managed security services are expanding now into other areas like Internet data, mobile, web and cloud-based ICT internet of things (hereafter, IoT) services and business models. People are connected to others and with things as well and expect always-on connectivity. It is expected to see trust ICT solutions from whole value chain, not only devices and networks but also applications and services. The European Union’s focus on trust and security in “Europe 2020 Strategy”, researches about the trust in projects of FP7’s UTrustIT, ABC4Trust and USA’s application of trust and security on industry level (NIST and DARPA), research about trust technology in projects like “Smart America” and HACMS are verifying the importance of the trust and security in the e-Commerce, SocialNetwork Service (SNS), IoT services and so on.

In business area, some leading firms are pursuing the same way in Financial technology (Fintech) area. Despite of such efforts of leading companies, recent big data business models are not trusted by consumers. There is ‘mistrust’ in e-Commerce, cell phone, SNS, tele-health and so on.

The trust ICT (based) business model is a good strategic positioning that builds trust with internet consumers by enabling them to control and leverage their own personal data. In doing so, trust ICT business model gives internet service providers a sustainable business strategy for disrupting current business model as well as delivering a permission-based services. The trust ICT business model is a game-changing disruptive strategy that enables firms using big data to provide incremental trust improvements to existing big data deployment. To exploit customer data more comprehensively, businesses must develop a much greater level of trust with their customers. So, the primary concern of this study is to overcome the gap between the personal controllability of privacy and business benefits of information service in terms of human and information service related trust. In fact, before IoT world, people only think of the trust regarding human-human or human-service (information) relationship. The trust issue is occurring not only in human-human but also in machine-machine and human-machine and vice versa.

The purpose of this study is to present trust ICT business models. For this, it firstly will define trust and trust ICT and discuss the disruptive innovation as theoretical background. With this backdrop, it will formulate the analysis framework for creating the trust ICT business models by three types of asymmetries and analyze the business model characteristics and related use cases with new market disruption.

### **The concept of trust and trust ICT**

**The concept of trust:** According to Wikipedia retrieved on August 28, 2016, trust is related to the emotion and in social contexts, trust has several connotations (McKnight and Chervany, 1996). Definitions of trust by Mayer *et al.* (1995) and Bamberger (2010), refer to a situation characterized by the following aspects: one party (trustor) is willing to rely on the actions of another party (trustee) the situation is directed to the future. In addition, the trustor (voluntarily or forcedly) abandons control over the actions performed by the trustee. The trustor is uncertain about the outcome of the other's actions, they can only develop and evaluate expectations. The uncertainty involves the risk of failure to the trustor if the trustee will not behave as desired.

**The concept of trust ICT:** According to Mayer *et al.* (1995), human/service-related trust is beliefs that the other party has suitable attributes for performing as expected in a specific situation irrespective of the ability to monitor or control that other party. This human/service-related trust has three components of integrity, ability and benevolence. The integrity refers to the beliefs that the trustee adheres to a set of principles that the trustor finds acceptable. The ability is the beliefs that the trustee has the group of ability, skills and characteristics that enable them to have influence within some specific domain (Mayer *et al.*, 1995; McKnight *et al.*, 2002). The benevolence is the beliefs that the trustee will want to do good to the trustor aside from an egocentric profit motive.

McKnight *et al.* (2011) defined system/network related trust. It is the beliefs that specific technology has the attributes necessary to perform as expected in given situation in which negative consequences are possible. It also has three components of reliability, functionality and helpfulness. The reliability means beliefs that the specific technology will consistently operate properly. The functionality is beliefs that the specific technology has the capability, functionality or features to do for one what one needs to be done. The helpfulness is beliefs that the specific technology provides adequate and responsive help for users.

The trust ICT has been extended from human/service to system/network relation as IoT world is emerging. The trust ICT before IoT world has been viewed as a subjective expectation that an entity predicts about other entity's future behavior. However, the trust ICT in IoT world can be viewed as the expecting performances that a thing or a system will accomplish a given task in an expected manner to fulfil its intended purpose.

In the new ICT environment with IoT, "trust provisioning is an integral function for the physical, cyber and social trust which provides a valuable method to minimize the risks through identifying trust characteristics of entities" by 'New Recommendation ITU-T Y.3052'. According to this ITU-T recommendation, using trust provisioning, it can develop trust ICT for better quality of services and experience by minimizing risks. The trust attributes of the trust worlds can be divided into the direct and indirect trust because the trust can affect the preference of an entity to consume a specific information, solution and network service offered by another entity. Those services can include security and privacy.

Coming from security perspective, trust ICT is the expectation that a system or solution will faithfully behave in a specific manner to fulfill its intended purpose. It means, the physical and cyber trust is generally supported by software and hardware-based solutions. The trust worthiness attributes categorized by Mayer *et al.* (1995) and McKnight *et al.* (2011) are suitable for these: Ability integrity, benevolence, reliability, functionality and helpfulness. Those attributes represent trustworthiness which can be applied to ICT infrastructures.

Many attributes have been clustered into three main attributes of ability integrity and benevolence by 'New Recommendation ITU-T Y.3052' (Anonymous, 2017) as follows: The ability enables an entity to have influence within some specific contexts. It is specific because the trustee may be highly competent in some technical area, affording that person is trusted on tasks related to that specific area. The sub-attributes related to this are robustness, safety, stability, scalability and reliability. The integrity is the quality of being honest and fair in the social world and the state of being complete in cyber and physical worlds. In terms of information integrity means that information of an object is prevented from being modified. The sub-attributes related to this include completeness, consistency, accuracy, certainty and recency. The benevolence is the desire to do well to others, working together for a common benefit when trustor has an interaction with trustee. It is also the extent to which a trustee is believed to do good to the trustor. The sub-attributes related to this are availability assurance, relevance and credibility.

Coming from privacy perspective, the trust is a more subjective expectation that an entity has about another's future behavior. This is indirect trust. It is formed from the judgment about the context and third party reputations or recommendations. It is deriving from the experience gained through previous interactions with the trustee and

the recommendation gained through the global reviews on the trustee. This is important in a circumstance where information to estimate trustworthiness attributes are not available at first-hand.

The experience is a personal observation considering only interactions from a trustor to a trustee. It is achieved by accumulating state of the interactions among entities over time. The reputation is a public assessment of the trustor regarding the trustee's prior behavior and performance and it is evaluated based on accumulated experiences of trustors about the trustee. To acquire trust information based on the reputation of a trustee, two kinds of information are necessary to examine: the previous trust transactions from all entities to the trustee and the relationship between a trustor to the trustee.

## MATERIALS AND METHODS

### Theoretical background and research questions

**Disruptive innovation:** There are three innovation models to creating new-growth businesses: sustaining innovation, low-end disruption and new market disruption (Christensen and Raynor, 2003). The sustaining innovation does not create new markets or value networks but rather only evolves existing ones with better value, allowing the firms within to compete against each other's sustaining improvements. However, disruptive innovation creates a new market by applying a different set of values which ultimately overtakes an existing market. There are two types: the low-end disruption targets customers who do not need the full performance valued by customers at the high end of the market. The new market disruption targets customers who have needs that were previously unserved by existing incumbents. The characteristics of each innovation models are presented in Table 1.

**Research questions:** There are some mistrust drivers. The first is privacy infringement. The endless supply of big

brother stories is shifting people's views on privacy and data making them more open to tracking privacy products. Government program used to collect internet user's material including searches, the content of e-mails, file transfers, IMs and live chats. The second is security breaches. The growing regularity of news reports about online security breaches is likely to lead a higher proportion of the population to change their behavior. Consumers are looking for improved security providing richer opportunities for security and privacy player and both combined. The third is government mass surveillance. The 'PRISM' revelations provide users with tangible evidence that the surveillance has been outsourced to a dozen of the Internet majors. In the middle of the mistrust, there is an imbalance of power. In corporation side, there are information overload, sophisticated analytics, contract control, transaction clarity, vendor price reference, data control and so on. In the consumer side, there is information scarcity, no contract control, transaction obscurity, now consumer price reference, no data power and so on. Such asymmetries give the firms power over consumers Table 2. They put individuals at a disadvantage and mistrust results. These are built on by service reflecting the imbalances of internet power (Little, 2014).

The result of the mistrust is the asymmetric internet. In information asymmetries, firms have an overload of user information but consumers suffer information scarcity in terms of their own data. In solution asymmetries, the firms have sophisticated analytics for optimizing customer lifetime value but consumers have no analytics for minimizing vendor lifetime cost. In control asymmetries, consumers are comparatively powerless to control the collection and use of their personal data, firms and governments have all the control.

Trust ICT business model is a positional strategy building trust not only with consumers by enabling their control of their own devices and data but also making

Table 1: Three approaches to creating new-growth businesses

Dimensions	Sustaining innovations	Low-end disruptions	New market disruptions
Targeted performance of the product or service	Performance improvement in attributes most valued by the industry's most demanding customers. These improvements may be incremental or break-through in character	Performance that is good enough along the traditional metrics of performance at the low end of the mainstream market	Lower performance in "traditional" attributes but improved performance in new attributes-typically convenience
Targeted customer or market application	The most attractive (i.e., profitable) customers in the mainstream markets who are willing to pay for improved performance	Over-served customers in the low end of the mainstream market	Targets non-consumption: customers who historically lacked the money or skill to buy and use the product
Impact on the required moneybusiness model (processes and cost structure)	Improves or maintains profit margins by exploiting the existing processes and cost structure and making better use of current competitive advantages	Utilizes a new operating or financial approach or both, a different combination of lower gross profit margins and higher asset utilization that can earn attractive returns at the discount prices required to win business at the low end of the market	Business model must make at lower price per unit sold and at unit production volumes that initially will be small. Gross margin dollars per unit sold will be significantly lower

**Table 2: Three types of asymmetries in big data business model**

Types	Contents
Information and service (price/transaction) asymmetries	Corporations have an overload of user information but consumers suffer information scarcity in terms of their own data and that relating to corporations Corporations know the costs and decide the price in terms of personal data currency but consumers have no price reference point for or clear perceived value of many online services Corporations decide what services to offer and what data to take but consumers don't know what amount of personal data is fare trade for what amount of services
Solution asymmetries	Corporations have sophisticated data analytics for optimizing customer lifetime value but consumers have no data analytic for minimizing vendor lifetime cost which is the flip side of customer lifetime value
Control asymmetries	Corporations have all the control of devices, sensors and related data collection and use but consumers are comparatively powerless to control of those

**Table 3: Analysis framework**

Three asymmetries of internet	Representative risks of social, cyber and physical world	Trust attributes of characteristics of new market disruption		
		Product/Service	Customer/Market	Process optimization
Information	Risks in social world Private information on SNS is propagated to others AI (Artificial intelligence) and social IoT mimic human	Simplicity and convenience Experience Reputation	Lack of the money or the skill Experience Reputation	Making money at lower price per unit sold Ability Integrity Benevolence
Solution	Risks in cyber world Big data analytics can pose critical privacy issue. Abused use of consumer data for data analytics	Simplicity and convenience Experience Ability Integrity Benevolence	Lack of the money or the skill Experience Ability Integrity Benevolence	Making money at lower price per unit sold Ability Integrity Benevolence
Control	Risks in physical world Components are resource-constrained, computation-limited. Poor security mechanisms are attacked easily. Devices, sensors, data collection and use are not recognized by user	Simplicity and convenience Experience Ability Integrity Benevolence	Lack of the money or the skill Experience Ability Integrity Benevolence	Making money at lower price per unit sold Ability Integrity Benevolence

ecosystem with business partners by enabling their creation of their products and services. The trust ICT gives companies a new business strategy for disrupting the legacy economy and delivers a more permission based data ecosystem and profitable services with trust attributes such as integrity, ability, benevolence, experience and reputation. The analysis framework is formulated like Table 3. It focuses on industrial background of three asymmetries like information asymmetries in product and service level, solution asymmetries in software level and control asymmetries in hardware and network level.

## RESULTS AND DISCUSSION

Table 4, trust ICT business models by 3 asymmetries of Internet and examples are proposed. To solve the problem of information asymmetries, ephemeral messaging application, reputation related services and ID management solutions are recommended. In ephemeral messaging services, messages are deleted and disappeared after recipients read them. As of July 2015, there have been lots of companies with similar business models such as Ansa, BBM, Burn Note, Bolt of

Instagram, Clipchat, Confide, CyberDust, Meerkat, Mirage, Periscope, Silent Text, Slingshot of Facebook, Snapchat, TigerText, Wickr, Yovo and so on. Their offering features various: SMS/IM, photos, videos, files, stickers, location, live-streaming, etc.

The reputation services provide privacy and reputation management for private individuals, their families and their businesses. After the first business model 'reputation.com' in 2006, lots of the similar reputation management applications came to the market. There have been top 25 services in the world as of February 2013: Reputation.com, Google Dashboard, Naymz, BrandsEye, Trackur, WhosTalkin, Yasni, Technorati, TweetBeep, BackTweets, WhoLinkstoMe, BoardTracker, Barracua labs, Lookup Page, Yext, FriendFeed, Watch That Page, SiteMention, Boardreader, Twenty Feet, Klout, Hyper Alerts and HubSpot' Marketing Grader.

Lastly for optimization of business model process, the ID management solution is valid as software as a service and it provides simplified identification methods using various technologies such as simple PIN code, onetime password, etc. Several large vendors are offering telco-specific identity management products

Table 4: Trust ICT business models by 3 asymmetries

Asymmetries of internet trust ICT	New market disruption related trust ICT business models with use cases		
	Product and service	Customers and market	Process optimization (B2B)
Information asymmetries ↓ Social trust	Ephemeral messaging app: TigerText, Snapchat, Ansa, BBM, Bum Note, Periscope, Bolt (Instagram), Meerkat Clipchat, CyberDust, Mirage, Silent Text, Stories (Facebook)	Consumer reputation management: Reputaation.com (former repotation defender), Integrity defender	ID management (B2B): Unbound ID Secure key
Solution asymmetries ↓ Cyber trust	e-mail data management app: MyKolab.com, Runbox, Countermail	Consumer IoT data management: Home automation (Nest) Home security (Dropcam)... Energy efficiency (AlertMe, green energy, options)	IoT management (B2B): Xively
Control asymmetries ↓ Physical trust	Device and companion app: Door lock (UniKey door), Health and diet (Happy Fork) Hygiene (Zubo)...	Consumer cloud storage management: Dropbox	Cloud management (B2B): OnApp, Orange Le Cloud, BT Assure Ethical Hacking for assure ethical hacking For finance, here (Nokia)

and solutions. Trusted brokers of information between e-Commerce providers and customers. Unbound ID is one of them to offer a solution that addresses data privacy to help telecommunication companies monetize identity data and build new revenue models around this information.

To solve the problem of solution asymmetries, Email data management, consumer IoT data management and IoT management for companies are recommended. The Email service provides security and privacy Email exchange methods using cryptographic technologies. In terms of e-mail management, a Swiss application service, MyKolab offers a lite version of its services, starting \$5 per month. By December 2013, it began accepting Bitcoin for user convenience. In Switzerland, abusing data is a criminal offence. Even if the CEO of a hosting business would learn of abuse among their staff and not report it to the proper authorities, they would likely look at jail time. Unlike in the US, all requests must go through a judge and be publicly documented in anonymized form and with proper attribution to the criminal code. Secret service has been explicitly stripped of all powers inside the country and there is no other legal way for foreign powers to obtain the data than through the international assistance treaties where requests for information must hold up under Swiss law.

The consumer IoT data management services and companies can be exemplified in connected home business model in the areas of automation, security and energy efficiency. Nest acquired by Google is a good use case as connected thermostat with remote control capabilities. IoT platforms can be as platform as a service for the business model optimization. For example, Xively provides the possibility to analyze and visualize the internet of things. It can be used to interconnect different devices over the internet and can store a history of measured values and can display it with graphs, etc.

## CONCLUSION

To solve the problem of control asymmetries, device and companion app, consumer cloud storage and cloud management for companies are recommended. In terms of personal cloud, cloud storage service provides additional security mechanisms for authentication to help ensure users are protected against data or credential breaches. Dropbox as cloud storage provider invests in security again by adding security-key authentication to help ensure users are protected against data or credential breaches when they log in to their accounts.

For optimizing business model process, the personal cloud can be as software as a service. It provides personal cloud as SaaS to other companies for developing a solution to synchronize any data with any connected devices. Cloud as infrastructure as a service provides trusted cloud as IaaS to other companies which develop various applications on cloud. OnApp IaaS Cloud Management Platform (CMP) for Small to mid-size Hosting Service Providers (HSPs) is a good example. HSPs can sell their IaaS CMP-managed resources on the OnApp Market, starting with CDN in 2011. The 3rd parties can use OnApp's available (under the open source GNU General Public License V 2.0) interface to its OnApp Market to enable anybody, not just those using OnApp Software, to access this market.

## ACKNOWLEDGEMENTS

This research was supported by Institute for Information and Communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) [R0190-15-2027, Development of TII (Trusted Information Infrastructure) S/W Framework for Realizing Trustworthy IoT Eco-system].

## REFERENCES

- Anonymous, 2017. New recommendation ITU-T Y.3052. Information Technology University, Lahore, Pakistan.
- Bamberger, W., 2010. Interpersonal trust attempt of a definition. Master Thesis, Technical University of Munich, Munich, Germany.
- Christensen, C.M. and M.E. Raynor, 2003. The Innovator's Solution. Harvard Business Press, Boston.
- Little, M., 2014. Personal data and the big trust opportunity. Ovum Ltd., London, UK.
- Mayer, R.C., J.H. Davis and F.D. Schoorman, 1995. An integrative model of organizational trust. *Acad. Manage. Rev.*, 20: 709-734.
- McKnight, D., V. Choudhury and C. Kacmar, 2002. Developing and validating trust measures for e-commerce: An integrative typology. *Inform. Syst. Res.*, 13: 334-359.
- McKnight, D.H. and N.L. Chervany, 1996. The meanings of trust. Master Thesis, University of Minnesota, Minneapolis, Minnesota.
- McKnight, D.H., M. Carter, J.B. Thatcher and P.F. Clay, 2011. Trust in a specific technology: An investigation of its components and measures. *ACM. Trans. Manage. Inf. Syst.*, 2: 12-25.