Latest R&D on Security Technologies at Fujitsu Laboratories

● Hiroshi Tsuda ● Ken Kamakura

Digital co-creation is underway mainly in relation to data, which is being referred to as the new oil of the 21st century. Meanwhile, new challenges are also emerging, such as countermeasures for cyber attacks, which are expected to intensify due to the utilization of the IoT, compliance with regulations relating to personal data, and ensuring the reliability of data to be fed to AI. Security technologies are raising expectations as technologies that support the trust of humans, data, and systems. Fujitsu Laboratories is conducting research and development in the three core areas of authentication/authorization, data security, and cybersecurity for the purpose of supporting safety and security of all customer businesses. This paper first outlines the security technologies that Fujitsu Laboratories is working on. Next, as a topic of the latest research, it describes a technology to ensure the trust of data by making use of blockchain technology.

1. Introduction

The 2011 World Economic Forum report stated that "personal data will be the new 'oil'—a valuable resource of the 21st century."[1)] In digital business in the future, industrial and personal data will be traded across countries, industries, and companies just like oil. It is assumed that those data will be processed with data analysis and AI technology to produce new digital co-creation. With these changes in data utilization, consideration must be given to new threats and risks. Issues like those described below, which should be resolved with security technologies, are also on the rise recently.

1) Borderless security measures

Data are not only held by one company but are now also used by multiple organizations for digital co-creation, which has brought changes to approaches on measures against cyber attacks. In dealing with increasing attacks, including the utilization of the IoT, the idea of security at organizational boundaries as in firewalls and intrusion detection and prevention systems (IDPSs) has limitations. Therefore, with attacks and invasions assumed, measures that allow for quick borderless implementation of detection and response should be considered standard. Another required approach is the minimization of risks in the event of data leaks through the use of anonymization and data protection technology.

2) Compliance with new regulations and guidelines

It should be noted that the tightening of legal regulations and guidelines has created the need for careful handling of data across organizations and countries according to the type of data. The National Institute of Standards and Technology (NIST) has established guidelines (SP 800-53 and 171) for classified information (CI: state secret level) and controlled unclassified information (CUI: important information), which also provide the conditions for government procurement.

A series of laws on personal data have also been enforced. These include the Amended Act on the Protection of Personal Information enforced in 2017 in Japan, the Cyber Security Law in 2017 in China, and the General Data Protection Regulation (GDPR) in 2018 in the EU.

3) New risks posed by AI

One issue specific to AI, such as with deep learning which uses a large volume of learning data, is the reliability of learning data. In one case that occurred in 2016, Tay, a chatbot developed by Microsoft, output inappropriate results due to inadequacies in the input data. A

technology referred to as adversarial examples has also emerged that causes erroneous judgments in image recognition results by adding noise to image data.

In the future, attacks such as data terrorism on AI-embedded systems should also be recognized as a risk. In addition, AI itself also requires explainability, which is the visualization of how results have been obtained, and ethical measures be implemented. In addition, how to ensure reliability and transparency of data to be fed to AI must be considered from the viewpoint of security.

4) Need for new trust model

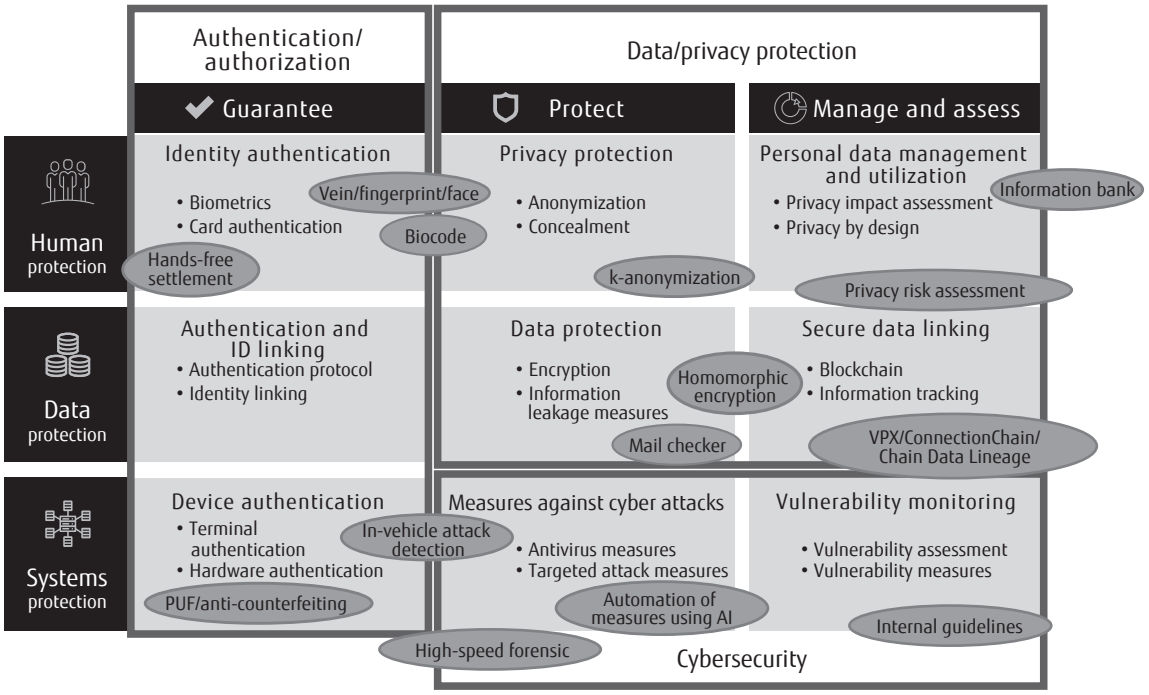
The concept of trust in humans and organizations is also beginning to change as digital co-creation activities are conducted by multiple organizations across countries. While trust was secured in the past by assuming a reliable third party using technologies such as a public key infrastructure (PKI), a mechanism in which participants support mutual trust such as a blockchain is now also effective in supply chains across countries and industries.

In response to this diversification of threats and risks, security technologies are expected to provide measures roughly in two directions. One is a technology for providing efficient protection by utilizing AI and automation technology, including a response to the present shortage of security personnel that support measures against cyber attacks. The other is an aggressive security technology that reduces new risks such as AI and legal regulations and enables digital co-creation.

This paper outlines Fujitsu Laboratories' defensive and aggressive security technologies and presents advanced technologies from the two perspective of cybersecurity making use of AI technology and data security to support digital co-creation.

2. Security to support digital businesses

Fujitsu Laboratories roughly classifies security technologies into three categories: authentication and authorization technology for the guarantee of humans and things; data protection technology for the protection and management of humans and data; and cybersecurity technology for the protection and management of systems. **Figure 1** shows an overall picture of security



PUF: Physically unclonable function
VPX: Virtual private digital exchange

Figure 1
Security technology matrix.

technology being developed by Fujitsu Laboratories. Humans, data, and systems are shown in the vertical direction as targets of protection, and three types of defense methods are shown in the horizontal direction. For example, there are biometric authentication technologies such as palm vein authentication as a technology for identity authentication, encryption and anonymization for data protection, and blockchain for data management.

2.1 Diversifying defensive security

Initial measures against cyber attacks were mainly entrance measures to prevent attacks on organizations by using firewalls, etc. However, as targeted email attacks (Advanced Persistent Threat attacks) and other cyber attacks are becoming increasingly sophisticated, it is impossible to block all cyber attacks at the entrance. This has increased the importance of ex-post measures assuming infection with malware.

The Cyber Security Management Guidelines[2] of the Ministry of Economy, Trade and Industry point out the necessity of constructing a system prepared for cyber attacks and recommend creating response and recovery systems.

In the future, response to the IoT will be indispensable for defensive security to support customer business continuity. The IoT, in which everything is connected to the Internet, requires an approach different from that of conventional cyber attacks according to the situation of application.

In constructing a system that utilizes the IoT, a combination of sensors from different vendors and the ensuring of security of the system as a whole are required. To detect vulnerabilities in IoT devices, Fujitsu Laboratories has developed a fuzzing technology intended for IoT devices.

In mobility (connected cars), response to real-time attacks on running cars is the first requirement. Fujitsu Laboratories has developed a technology that uses an automotive electronic control unit (ECU) for real-time detection of attack messages inserted in Controller Area Networks (CAN), an in-vehicle network technology.[3] In mobility, it is necessary to implement these emergency measures in automotive equipment at the same time as long-term measures by centers that aggregate information from each vehicle to apply online updates for individual models.

In factory and industrial control systems, cyber attacks on operational technology (OT) departments have become apparent as automatic control via OT advances. In factories, stopping production lines leads directly to business losses. Therefore, it is not always possible to immediately stop the equipment infected with malware, and careful response is necessary. The expectations are also high for AI technology, which can assist experts with their work in responding to such attacks.

2.2 Aggressive security for digital co-creation

In digital co-creation activities across different organizations, it is necessary to understand whether or not the identity of the other party is genuine and how to guarantee the reliability of authentication. Security technology can also be used for aggressive activities to resolve these issues and create new businesses.

To ensure the reliability of identity authentication, we have developed biometric authentication technology including palm vein authentication, a Fujitsu proprietary technology. While conventional palm vein authentication was capable of authenticating one person out of about 10,000, combined with face recognition, new technology is able to authenticate out of about 1 million people. This has made possible non-contact authentication and settlement without the need for devices such as smartphones or cards, even at large-scale events. For details, refer to the paper "Biometric Authentication Technology Facilitating Protection and Management of Biometric Data" in this issue.

Data security must be considered from three perspectives: confidentiality (C), integrity (I), and availability (A). Blockchain in particular is raising expectations as a technology that realizes I and A. The technology for using the blockchain technology to manage the history of data across different companies will be described in Section 3. For the ConnectionChain technology that links blockchains, refer to the paper "Security Technology ConnectionChain for Securely Linking Blockchains" in this issue.

3. Data security to support digital co-creation

This section describes security technology with a focus on data privacy protection that supports the reliability of digital data.

3.1 Data distribution technology for digital co-creation

In digital co-creation, where different organizations from industry, academia, government, etc. are mutually connected to create new values and services, digital data circulate in cyberspace, forming a supply chain of the data. In addition, the reliability of the data fed to AI is important in the utilization of AI technology. It is assumed that, moving forward, history will be required for data in the same way that raw material labeling is essential for ensuring the reliability of processed food. For this reason, there is a need to be able to verify who created the data, with what process it was created, and from what data it was created. When the utilized data includes personal data, verifiability of whether they have been collected with individual consent is an important requirement.

Based on this background, Fujitsu Laboratories has developed data history management technology that allows for the grasping of histories, such as the source and path of the data, in a centralized fashion.[4] The following describes the technology of centralizing the management of consent for distributed personal data to allow simple and safe distribution of personal data based on individual consent.

1) Issue

Standards relating to the distribution of personal data between companies include "OAuth" for authorization and "User-Managed Access (UMA)," which is an access management protocol based on OAuth. They are both designed for individuals. For example, it is possible to provide another medical institution with medical information by acquiring the patient's consent. However, applications involving collective transfer of personal data owned by a company to another organization require a new design.

Figure 2 shows a typical configuration of OAuth and UMA. UMA is a model that authorizes data on a per-user basis and provides it to a third party. If multiple communications generated between each server and client are repeated as they are for the number of persons, the number of messages becomes enormous. This results in a large amount of processing and traffic volumes, whose reduction in turn becomes an issue.

2) Developed technology

In order to resolve the issue mentioned above, we have developed a method in which UMA is extended to allow the embedding of data formats and attribute specifications to handle multiple data groups virtually as data for one person and assign the data groups to a token. As a result, data for more than one person can now be collectively acquired in two sequences regardless of the number of persons while taking advantage of the safety of access control that UMA is originally equipped with. However, this extension causes vulnerability to attacks in which fraudulent links are sent in targeted email to acquire data. Accordingly, we have added a token verification function.

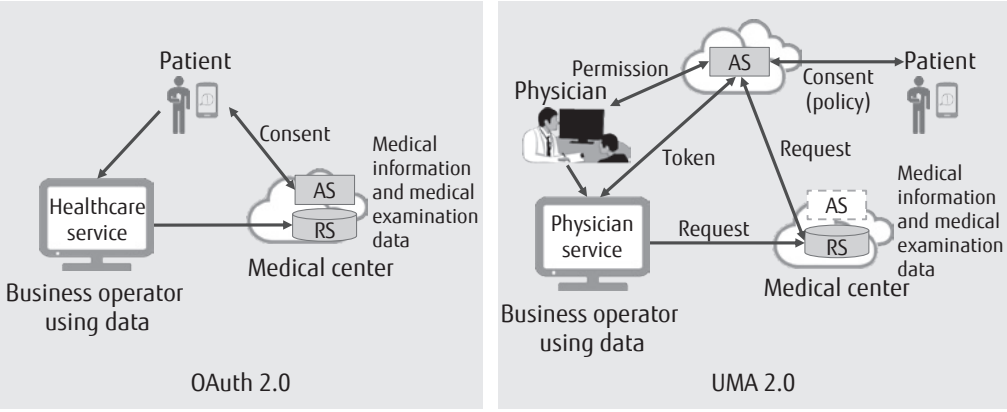


Figure 2
Configuration example of OAuth and UMA.

3.2 Effect of developed technology

With UMA, verification of the results of consent is done on the authorization server. Therefore, for collective acquisition of data between companies using the developed technology, only the data with consent are transferred. The consent information and personal data access history held in the authorization server are managed by a blockchain and difficult to alter. This management makes use of Fujitsu's blockchain cloud service "FUJITSU Intelligent Data Service Virtuora DX Data Distribution and Utilization Service."

We have also built an experimental consent portal that can be used to acquire individual consent. This saves service providers the need for building their own consent acquisition application and consent information management system. In addition, operations have been centralized from the viewpoint of usability to offer ease of handling.

One application example of this technology is the utilization of driving habits data acquired by a data brokerage company from motor companies and car rental companies (**Figure 3**). To this driving habits data, data necessary for driving analysis can be added, such as map data and traffic data for creating a driving model of a driver. Telematics insurance service can calculate the insurance price based on it and provide a personalized car insurance service. Users can verify the basis for the calculation, such as which of the data collected with their consent to provision was used to calculate the insurance price.

4. Conclusion

This paper described Fujitsu Laboratories' latest technologies in defensive and aggressive security to support digital businesses.

In addition to responses to new challenges such as compliance with legal regulations of data, countermeasures to the leakage of personal information, and reliability of data fed to AI, cyber attacks including the IoT are increasing and causing significant damage. Meanwhile, there is the reality of a shortage of security experts. The new security technologies using AI and blockchains described in this paper are technologies that expand the capabilities of these security experts and realize the trust of humans, data, and systems. We intend to continue with research and development ahead of its commercialization.

References

1) World Economic Forum: Personal Data: The Emergence of a New Asset Class. *http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf*
2) Ministry of Economy, Trade and Industry: Cybersecurity Management Guidelines Ver 1.1. *https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guidelines_v1.1_en.pdf*
3) Fujitsu Laboratories, Fujitsu: Fujitsu Defends In-Vehicle Networks with New Technology to Detect Cyberattacks. *https://www.fujitsu.com/global/about/resources/news/press-releases/2018/0124-02.html*

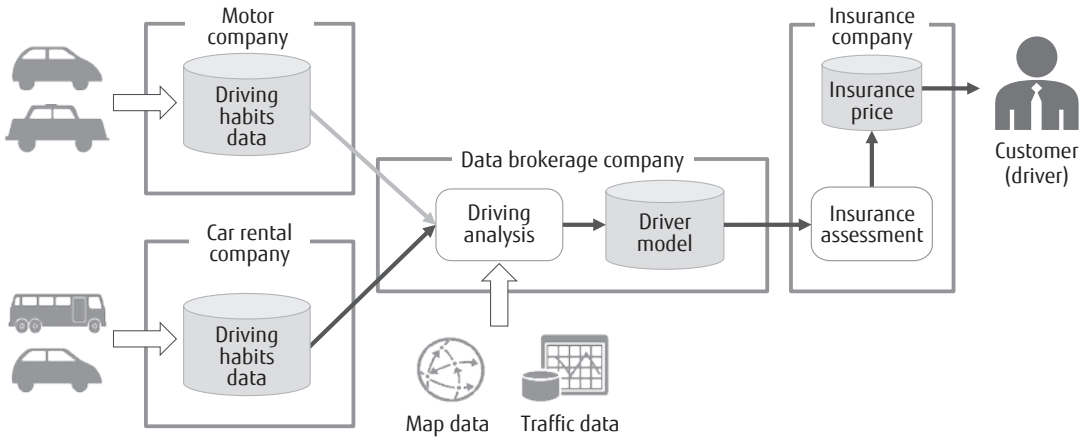


Figure 3
Automobile insurance based on driving history.

4) Fujitsu Laboratories: Fujitsu Develops Technology to Improve Reliability of Data Distribution Across Industries. *https://www.fujitsu.com/global/about/resources/news/press-releases/2018/0920-02.html*

Hiroshi Tsuda
Fujitsu Laboratories Ltd.
Dr. Tsuda is currently engaged in research and development on data security, digital identity, and blockchains.

Ken Kamakura
Fujitsu Laboratories Ltd.
Mr. Kamakura is currently engaged in research and development on the application of data security and blockchains.