Knowledge Creation of Adaptive Learning on the Blockchain System
-Collaborative Cloud Educational System-

Mayumi Hori, Chuo University, Japan
Masakazu Ohashi, Chuo University, Japan

Abstract
The major difference of the networked society from the conventional analog society is its potential of increasing the continuity of time and space. That is, it transcends the boundaries between individuals and organizations, private and public sectors, family and work, business and pleasure, producers and consumers, the national and local governments, different disciplines and so on. With this continuity based upon an advanced ICT infrastructure, tacit knowledge, which is the most difficult yet valuable type of knowledge to be transmitted that is gained through personal experiences and stored within individuals, has better chances to be transferred and shared. Therefore, building a platform to make tacit knowledge more accessible and sharable in the society is essential. In this paper, we would like to discuss Adaptive Collaboration, which integrates different systems and applications into one comprehensive system. The Adaptive System holds the potential to connect different entities such as corporations, university lecture, and Project Based Learning to enable the Adaptive Learning (AL) which is critical to meet the increasingly diverse needs of the Ubiquitous Society. The structure of this paper is as follows: First, we introduce the AL and discuss the potentialities of application of the Cloud System based on the Block Chain Technology. Second, we refer the experimental pilot study on the AL and provide further observation for applying the AL. Third, we discuss how this Society utilizing the Cloud Services based on the AL would affect the lectures and AL.

Keywords: Block Chain, Adaptive Collaboration, Adaptive Learning, Cloud System

iafor
The International Academic Forum
www.iafor.org

Introduction

The future direction, and agendas for e-Local Governments are to re-build the deteriorated fiscal structure in public administration with innovative management minds, and to promote administrative autonomy by decentralizing the society, while many Local governments suffer from their depreciated financial situation. Under these situations, IT systems should be mutually worked between central and local government. It avoids overlapping investments of the ICT utilization and development by determining the development methods. In this paper, we discuss the potentialities of standardization for promoting the certification of digital contents and originality .in order to swiftly and appropriately satisfy a central and local organizations, further development and utilization of IT and its infrastructure in the local municipalities.

In our modern clock-ruled culture, it is not too much to say that no society can exist unless based on "time". Computers, which are the key device of an information society, are equipped with high precision clocks to synchronize their entire circuit function. In an electronic environment or digital society built on computers, recordkeeping relates inevitably to the time that is ticked away by the clocks embedded in the computers. Time is thus the infrastructure of this information society. However, the importance of securing evidential authority of electronically determined time, and synchronizing clocks of multiple computers working in cooperation are not recognized enough.

To save the situation, a notion of time for the digital society should be properly defined and popularized, specifying the way and conditions of using it safely. Time Business Forum was established to diffuse the time notion for the digital society. We focused mainly on time-stamp use by national and local governments to produce a general study for both users and providers.

Currently, there are various services available that utilize the Internet. Additionally, more and more services are newly created to meet users' diverse needs by incorporating existing services and social infrastructures. Nonetheless, many of the existing services are often provided with specifications unique to each service provider, making it difficult or even impossible to integrate them with existing social infrastructures. Therefore, it is essential to develop a scheme that incorporates different services and infrastructures without boundaries of specifications.

Traditionally, many services were provided by locally connecting computers. However, with the rapid and widespread diffusion of the Internet, the demand for integration remotely or globally has increased. Consequently, there emerges an increasing need for the development of technologies that incorporate different systems. However, implementing the same technology used for connecting computers locally into a system connecting computers globally is costly and time consuming.

The social infrastructure is a wide concept, and it includes so many various entities. Today, not only information and communications technologies (ICT) including broadband networks and mobile phones but also the logistics and sales systems are prevailed as social infrastructures. Nonetheless, there are still few models that

transcend the difference of business types and industries, and connect them altogether to provide a new service.

For the demonstration experiment, we selected the Business to Consumer (B to C) model. The model we built aims to utilize different social infrastructures, and coordinates with other services regardless of their business types and industries to offer convenient and effective services for users. We developed the Adaptive Authentication System that provides user-centric services as well as the authentication system essential for coordinating different systems.

Project Based Learning (PBL) is an innovative instructional strategy that has been widely applied at educational institutions of variety of levels. PBL encourages students to engage in "real world" problem-solving investigations. It also allows students to autonomously conduct their study in a more constructive manner as well as develop the critical thinking skills of causal reasoning. Likewise, current Knowledge Management (KM) theories and practices have in many ways played equally important roles in corporations and educational institutions. KM and education share the same philosophies that play critical roles at many organizational levels that require an efficient understanding of their collective information and knowledge.

In this article, we would like to emphasize the importance of combination of PBL, KM, and Collaborative Learning on the Cloud and the incorporation of technology into education. We also would like to demonstrate how our approach enhances student skills and abilities by introducing case studies conducted at Chuo University in Japan. We describe the mechanism of human intellectual development and knowledge structuralizing process by studying topics in cognitive science as possible aids for new knowledge creation – categorization, metaphor, and metonymy.

In this paper, we introduce the Adaptive Authentication System and discuss its potentials in the new paradigm of the 21st century networked society. It is an innovative information technology system for knowledge creation based on the Cloud Computing and Time Authentication. It is a new system that produces dynamic and valuable interactions among human resources through sharing, interlocking, and collaborating with different types of knowledge.

Blockchain is at the center of attention. But, major applications of Blockchain are related to cryptocurrency. This created a snowball of hype, that over the course of months, brought us to a sorry state of our community, once driven by the ambition to enhance humans, by empowering freedom thanks to technology, but now driven by money being made by confusion." Then, We study a new application of Blockchain.The Internet has increasingly become important. As a result, official ID on the Internet is required. The purpose of this study is to propose online identity verification using Blockchain, decentralized system.

1. Key Technologies on Adaptive Collaboration Systems

1-1. Implications of the Study

In the Ubiquitous Society, open networked information systems are vital as they enable people to collaborate with others regardless of location and type of business. In that environment, we will experience shifts in our communications both in terms of quantity and quality. Not only "Human-to-PC," but a new pattern of "PC-to-PC" will expand the dimension of communications. The information we share with others will include not only textual information but a disparate range of data and information and including knowledge that is essential for decision making.

Therefore, the primal benefit of collaboration is the sharing of knowledge, information, and data with others. In order to realize this, there needs to be a space or "*ba*" where a variety of applications help users to produce new knowledge, information, and data that are appropriately shared and re-used among users. We conducted a demonstration experiment to examine technologies that are essential to build this knowledge sharing environment.

The information and knowledge sharing space has two distinctive attributions – static and dynamic. One is that it statically unifies the management of information and related behaviour, and the other is that it adds actions to make it adaptive to the dynamic operation processes. The stored data are structured for the purpose of re-use, hence it is also the "*ba*" that encourages knowledge recycling.

Since there are many possible operations imaginable that are suited for the Adaptive Collaboration, its goal is to provide users with a workspace to accomplish their own tasks instead of simply offering functions such as word processing or spreadsheet applications. The workspace may offer email and bulletin board services or document management services. The possibilities are infinite as it is also able to integrate specialized applications for each operation into the user interface.

1-2. Requirement and Purpose of the Study

For successful collaboration, it is essential that data, information, and knowledge are continuously stored and can be shared among many individuals. In order to do so, it is critical not only to build a reliable infrastructure and developed network, but also to consider how the data should flow on the network along with how the data should be applied and utilized. For certain fields, it is strongly preferred that contents still be usable without depending on specific applications or software, or when values are changed 100-200 years from today. That is, data and content need to be constantly viewed, utilized, and processed by many users. Furthermore, the system needs to be flexible enough for the distribution and re-use of data and content as they might be stored at dispersed locations at different times.

Therefore, the essential requirements for AC are the following: 1) users are geographically-dispersed and belong to different organizations, 2) knowledge information is easy to store and retrieve, and long-term information storage needs to be safe and secure, 3) knowledge information needs to be available for high-level

statistical processing and analysis, and 4) it operates uninterruptedly, and it is low in cost and highly-reliable.

The purpose of the study is to realize the real-time AC environment through data sharing. For this purpose, we conducted the following experiments: 1) a demonstration experiment on the Storage Management which enables users to share information located in the iDC storage, 2) a demonstration experiment on data management by applying XML Web Services into the real-time collaborative work system through data sharing ([13]2004 [11]2003a).

2. Adaptive Collaborative System

2-1. Adaptive Collaborative System

For ensuring the durability and universality of data, it is important to standardize a character encoding scheme and data structure as well as a system that reconstructs and personalizes data according to the need of a user. In terms of data structure, it is necessary to standardize data format that is both open and global for the purpose of information transmission and distribution across the world. In terms of personalization, it is indispensable to consider how to systemize knowledge so that a system could tailor and reconfigure data for each user depending on a situation to utilize stored data. Collaboration can be divided into three categories from the perspectives of a long term use, "ba" on the Internet, and application of the XML Web services technology into digital data: 1) intensive utilization of network infrastructure, 2) network utilization for information and knowledge, and 3) integrated utilization of distributed data in a large area.

For security of transactions and procedures taking place on the digital network, evidence of the existence of relevant facts and proof of document delivery are also necessary. Therefore, along with digital signature, time-stamp is essential to authenticate (guarantee) that a digital document existed at a certain time.

It is expected that time-stamp will be effective in the following functions and services:
• Evidence of the existence
To guarantee that digital contents existed at a certain point of time.
• Proof of delivery
To prove that a transmitted document has reached the recipient, as well as that the recipient have received the document. Also known as "delivery evidence" which is equivalent to delivery certificate used in existing postal service. This contributes to avoiding repudiation threat.
• Long storage of electrically signed documents

To secure authenticity of a digital contents over time by providing existential evidence. The proper time of document verification information is authenticated in order to cope with digital documents exceeding the PKC validity period or key algorithm compromised.

In order to realize this open and flexible data structure and information distribution, it is necessary to conduct demonstration experiments in the following ways:

- Providing and integrating an *Active* utilization environment and a *Static,* long term environment on the network, an *Adaptive* space.

MAN (Metropolitan Area Network + iDC (Internet Data Center)

- Building an environment with the XML Web Services technology that is independent of a system and application.

In order to examine the feasibility of these mentioned above, we conducted a demonstration experiment. First, we examined the possibility of collaboration among corporations, universities, and research institutions by building an information sharing environment prior to applying XML Web Services into the data management system which utilizes the information stored within the iDC. Second, we examined the effectiveness of the data storage system and evaluated whether the external applications are capable of high-level utilization such as its proficiency of producing knowledge out of information, presenting data effectively, and storing know-how. (Fig. 1,2)
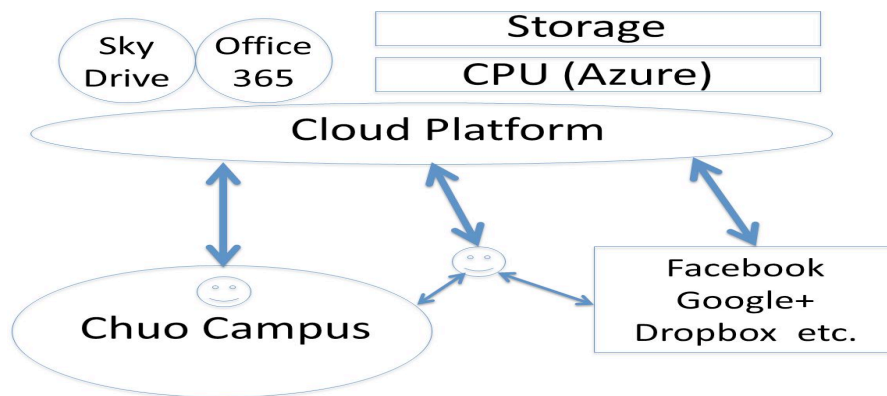

Figure1: Adaptive Collaborative Learning System1 （1st System of 2013−2015）[6]
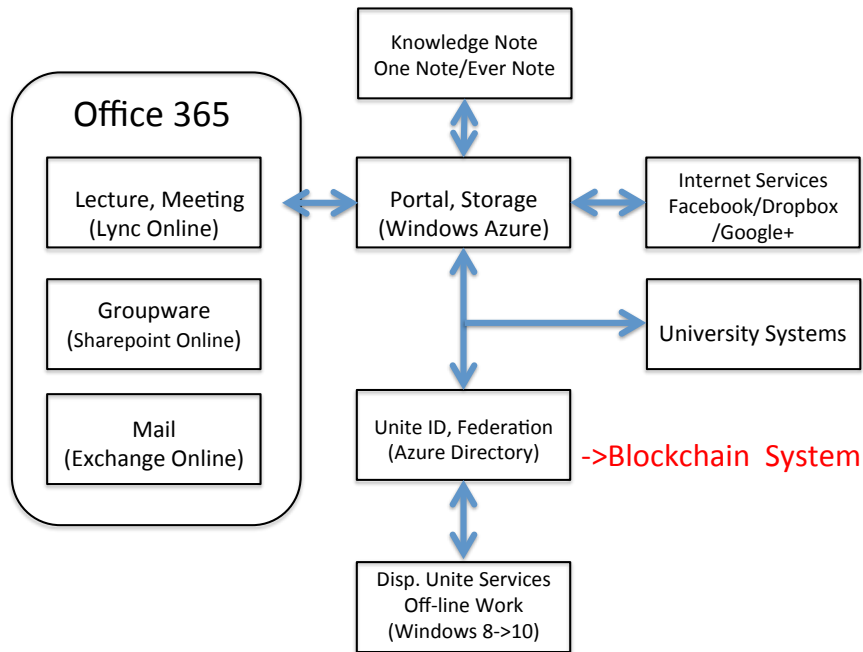
Figure2: Adaptive Collaborative Learning System2

2-2. Adaptive Collaborative Authentication

The demonstration experiment proved that real-time discussion with sharing data and resources among the geographically-dispersed teams was possible. Furthermore, we confirmed that it is possible to collaboratively edit and process image data between remote locations using a high-speed network.

For the future agenda, if we plan the long-term use of the system, it is necessary to consider how to manage the Web services and how to develop and spread its computer architecture in corporations. In other words, in order to administer the relationship between different Web services on the multivendor delivery platform, it is necessary to consider how to manage many different components involved in this system such as network operation management, service management, and Web Services management including ERP, CRM, SCM, EAI, and, EC.

Physically storing files and data and keeping them readable for a long time do not necessarily mean keeping them understandable for a long time. It is critical for a variety of systems to be able to cooperate in order to process diverse data while extensively accessing meaningful data. To facilitate this, it is essential to utilize a unified meta-standard technology such as XML and Blockchain , and to add autological, self-explanative description onto data themselves.

2-3 Time Authentication

As already mentioned, digital signature is a means to enable personal verification and content authenticity of digital documents, which are involved in transactions and procedures to be secured. For security of transactions and procedures taking place on the digital network, evidence of the existence of relevant facts and proof of document

delivery are also necessary. Therefore, along with digital signature, time-stamp is essential to authenticate (guarantee) that a digital document existed at a certain time([9]Ohashi,M.,2003a).

It is expected that time-stamp will be effective in the following functions and services:

- Evidence of the existence

To guarantee that a digital document existed at a certain point of time.

- Proof of delivery

To prove that a transmitted document has reached the recipient, as well as that the recipient have received the document. Also known as "delivery evidence" which is equivalent to delivery certificate used in existing postal service. This contributes to avoiding repudiation threat.

- Long storage of electrically signed documents

To secure authenticity of a digital document over time by providing existential evidence. The proper time of document verification information is authenticated in order to cope with digital documents exceeding the PKC validity period or key algorithm compromised.

3. Mechanism of Authentication on Blockchain System

Time Authentication provided the certify of originality of Contents and Blockchain provided the identity authentication of the distributed system.

3-1. Mechanism of Authentication using Hash Function

Time authentication infrastructure can be technically defined as a system infrastructure for providing standard time distribution, time-stamping, and other related services. The standard time distribution service is conducted by Time Authorities (TAs) in place of National Time Authority (NTA), while the time-stamping service provides evidence that a data item existed before a certain point in time, based on the time source distributed from NTA or TAs.

This chapter describes the mechanism of time authentication infrastructure, which supports time-stamping services. Time-stamping service systems (i.e. time-stamp token issuance and validation systems) described here are based primarily on the international standards such as RFC 3161 and ISO/IEC 18014.

3-2. Usual Time Authentication Service Model

The following paragraphs outline a time authentication service model applied to e-application system of the system.

・CA

Certification Authority, which issues NTA, TA and TSA with appropriate certificates or PKCs for digital signatures. Some time-stamping systems do not involve this player.

・TST verification player

Verifies the validity of time-stamp tokens. The entity of this role can be different depending on time-stamping system. TSTs based on simple protocol system can be verified on PKI by clients themselves. In the case of the TSTs based on linking protocol system, TSA, who issues the tokens, or some other third party becomes the player.

・Applicant

Students use applications, or the software and tools. They follow application formalities in communication with the application acceptance system of thesystem. They can make a request to TSA for time-stamps to prove their applications' existence. In the case of some trouble, they verify the validity of TSTs issued from the local government, by using the TST verification player.

・University

University providing application services for students, or the application system itself. Based on time-stamping services provided by TSA, the University gives time-stamps to application forms from applicants, acceptance notice, result notice and other documents produced during the application transaction. In the case of trouble, it verifies the validity of TSTs it has issued, by using the TST verification player.

The time authentication service model in bid / application business of an electronic local government
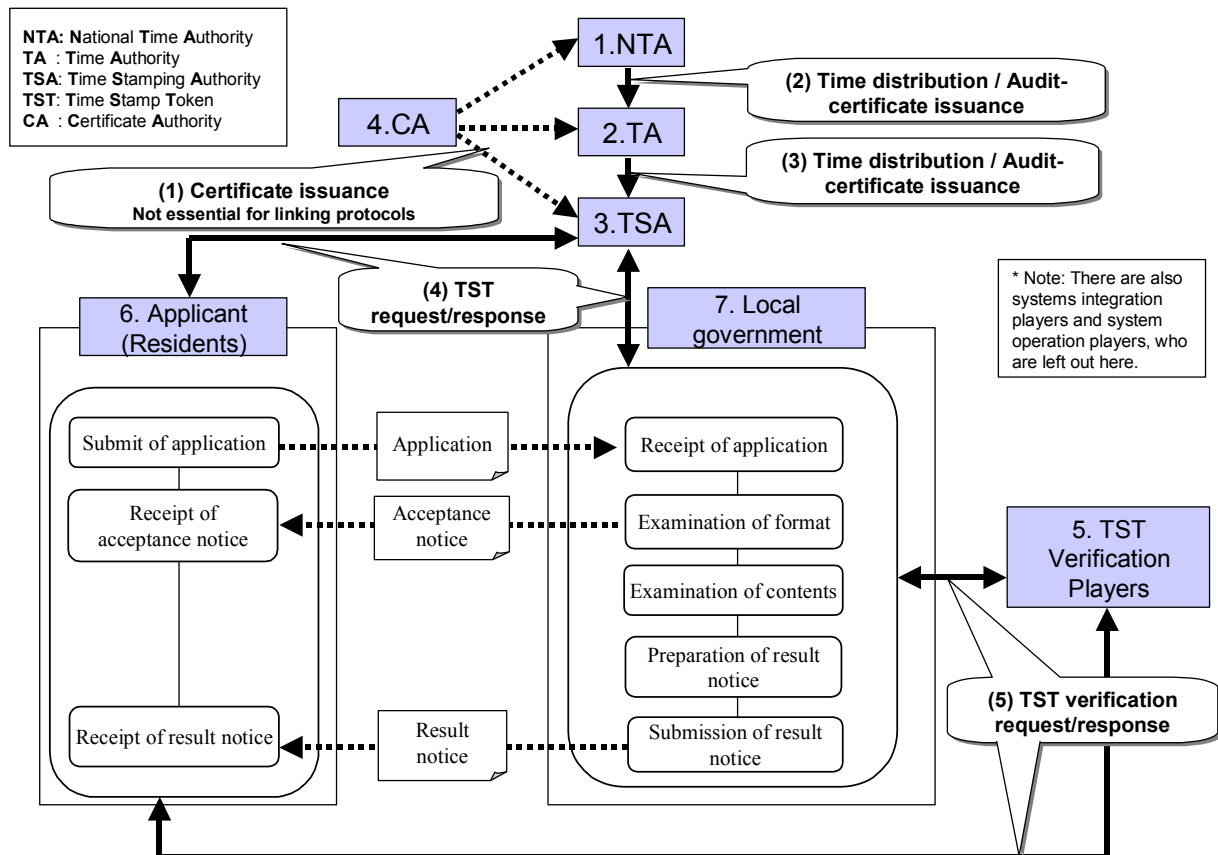
NTA: **N**ational **T**ime **A**uthority
TA : **T**ime **A**uthority
TSA: **T**ime **S**tamping **A**uthority
TST: **T**ime **S**tamp **T**oken
CA : **C**ertificate **A**uthority

1.NTA

(2) Time distribution / Audit-certificate issuance

4.CA

2.TA

(3) Time distribution / Audit-certificate issuance

(1) Certificate issuance
Not essential for linking protocols

3.TSA

* Note: There are also systems integration players and system operation players, who are left out here.

6. Applicant (Residents)

(4) TST request/response

7. Local government

Submit of application	Application	Receipt of application
Receipt of acceptance notice	Acceptance notice	Examination of format
		Examination of contents
		Preparation of result notice
Receipt of result notice	Result notice	Submission of result notice

5. TST Verification Players

(5) TST verification request/response

Figure 3 Time Authentication Service Model for E-application Transaction [23]

3-3. Blockchain System

We built a Blockchain System; 1.Make a Block, 2.Make a Chain, 3.Search a Chain, 4. Arrange a Chain, 5.Connect the System. Blockchain system included the hash function of certification. Blockchain identity verification is different from centralised identity verification relying on organization and system. Individual distributed authentication can manage easily the distributed system and the certificate contents.

Conclusion

To become widely approved in society, the time notion for an electronic environment needs to win public awareness, trust and daily opportunity as well as technical support. Given that the modern world is based on "time", an electronic/digital world can be based on an integral structure that authorizes "digital trace of time". We call the whole such structure as "time authentication infrastructure", establishment of which is the objective of this chapter. Through describing the feature, importance and effects of time-stamp as a trace of time given to digital documents/data stored for future use. Consequently, time-stamp users will know business application standards for appropriate time, documents/data, trace of time and certified originality of digital contents, while providers will be suggested service quality standards such as type and reliability of time-stamp they offer.

Our study proved the effectiveness of the Time Authentication to trusted e-Procurement to create new Secure services between Public Sector and Private Sector (Citizen). Though there are still issues to cope with outside of the realm of technology including accountability of each participants and the level of the service.

The Adaptive Collaborative Learning, which has drawn attention as a new network system that supports the future Ubiquitous Society. The ACL is capable of functioning with the legacy system that has been widely utilized in organizations while integrating a number of different applications seamlessly. With these beneficial features, more innovative business activities can be conducted such as sharing the order information across the organization, improving efficiency in CRM, risk management, delivery management, profit-cost management, cash flow accounting, balance sheet adjustment, account receivable factoring, updating and comparing the transition of sales, and making strategic decision and setting practical business goals.

The ACL is the most versatile system that facilitates to realize the AC in the Ubiquitous Society. For instance of incorporating the XML Web Services, since it is solely application/system independent, this also assists the flexible coordination with other systems and creates a seamless environment for the user hence it is highly functional as a core system.

We successfully proved the validity and effectiveness of the B to C model and Authentication Roaming Technology through the experiment that connected the multi-copying machine at a Seven-Eleven store and the system of Chuo University via the Internet. Though the incorporation of social infrastructures has long been led by the service providers, with the advent of the Authentication Roaming Technology, we can finally take a user-centric approach to incorporate social infrastructures and

provide safe and convenient services for users. This new approach will enhance the efficiency of various services and allow us to create new business models.

The Ubiquitous Society is a society grounded upon the collaboration around human knowledge within organizations and individuals. The biggest bottleneck of the ACL might not be the difficulties in developing the technologies and infrastructures. Rather, it might be the introverted and closed nature of human beings.

Acknowledgement

References

Dumortier, J. and Vandezande, N.(2013), Critical observations on the proposed Regulation for Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, ICRI Working Paper (06/2013), Interdisciplinary Centre for Law and ICT, K.U.Leuven, pp.1-20.

European Commission (2012), Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, ETSI TS 119 403, V1.1.1.

Government Office for Science (2016), Distributed Ledger Technology; beyond blockchain, UK Government Office for Science.

Hori,M.& Ohashi,M.(2005), Adaptive Collaborative Work and XML Web Services, Dr. Guah and Dr. Currie (Ed.), Internet Strategy: The Road to Web Services, Chapter VII, IRM Press.

Hori,M.& Ohashi,M.(2007), Knowledge Creation and Adaptive Collaboration Based on XML Web Services, Dr.Goran D.Putnik & Dr.Maria Manuela Cunha (Ed.), Knowledge and Technology   Management   Virtual Organizations: Issues, Trends, Opportunities, and Solutions,Chapterp.14,pp.292-305, IDEA Group Publishing.

Hori M.,Ohashi M. & Kurata N., (2016), The Adaptive Collaborative Learning Applying into The University Students -The Potential of the Cloud Services in the digital Revolution-, Proceedings 12th International Conference on Knowledge -Based Economy and Global Management, STUST Press, pp.187-193

Kawaguchi, N.(2018),Online Identity Verification Using Blockchain, Journal of Transformation of Human Behavior under the Influence of The Infosocionomics Society, Vol.3, pp.49-54.

Ohashi,M.& Nagai,M.(2001), Internet Data Center Revolution, Impress, Tokyo,Japan.

Ohashi,M.(2003a), Time Business, NTT Publication, Tokyo,Japan.

Ohashi,M.(2003b),Public iDC and c-Society, Kogaku Tosho, Tokyo,Japan.

Ohashi,M.(Ed.)(2003a),Knowledge-Based Collaborative Work, The Report of Supplementary Budget Project of the Ministry of Post and Telecommunications.

Ohashi,M.(Ed.)(2003b), The Report of Society for the Advance Study on e-Society, The Society of the Basis for e-Community.

Ohashi,M.(2004),The Time Authentication of Digital Contents, Journal of Policy and Culture Vol.11, Chuo University Japan, pp.69-85.

Ohashi,M.(Ed) (2004), The Report of the Advanced Studies for the Social Capital of e-Society, The Society of the Basis for the e-Community,Japan.

Ohashi,M., Sasaki,K. & Hori,M.(2004), On the Study of Knowledge Structualization and Adaptive process Based on Project Based Learning, Journal of Policy Studies Vol.11,The Institution of Policy and Cultural Studies, Chuo University,Japan,pp.55-78.

Ohashi,M & Hori,M.(2005),The Theory of Economics for Network Society, Kinokuniya Co.,Ltd.,Japan,pp.2-5,pp.106-118.

Ohashi,M.(Ed.)(2005), XML Web Services for Next Generation & A view of Citizen Centric, Kinokuniya Co.Ltd., Japan.

Ohashi,M. & Hori,M.(2009),Technical Perspective for the e-Health Care Management of Adaptive Collaboration Based on Authentication Roaming between Different Certificate Authorities, Chapter 7, pp.156-169 ,Handbook of Research on Developments in e-Health and Telemedicine: Technological and Social Perspectives, Medical Information Science Reference, Hershey ,New York.

Ohashi,M. & Hori,M.(2010), Certified Originality of Digital Contents by the Time Authentication,Chapter6,pp.67-80, Information Communication Technology Law, Protection and Access Rights; Global Approaches and Issues, pp.560., Information Science reference, IGI Global, Hershey, New York

Ohashi,M.,Sakimura,N., Sakushima,T. & Hori,M.(2010),On the Substantiative Experiment Study of Proxing Assurance between OpenID and SAML -Technical Perspective for Private Information Box Project of Japanese e-Government-,CCIS 110, Part2. Springer, pp.381-390.

Ohashi,M., Sakimura,N.,Fujimoto,M.,Hori,M., & Kurata,N. (2013), Technical Perspective of Authentication Policy Extension for the Adaptive Social Services and e-Health Care Management, Chapter 37, Handbook of Research on ICTs for Healthcare and Social Services: Developments and Applications, pp.719-726, IGI Global.

Satoshi,N. (2008), Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf''

Time Business Forum (Ed.)(2003), Time Ausentication Infrastructure Guidelines, Time Business Forum, Japan.