A Study on Design and Implementation of E-Discovery Service based on Cloud Computing*

Taerim Lee, Hun Kim, Kyung Hyune Rhee, Sang Uk Shin[†]
Pukyoung National University,
Busan, Republic of Korea
{taeri, mybreathing, khrhee, shinsu}@pknu.ac.kr

Abstract

In order to minimize time & cost for E-Discovery, many vendors have developed and released competitively their own service systems or software applied state-of-the-art technologies. Among them, Cloud Computing is one of the most exclusive skills as a computing infrastructure for E-Discovery service. However, these products actually do not cover all E-Discovery works that have to be done and have many drawbacks & considerable limitations. So, this paper proposes a new type of E-Discovery Service Structure based on Cloud Computing called EDCS(E-Discovery Cloud Service) to make the best use of its advantages and overcome the limitations of existing E-Discovery solutions. Simply put, the goal of EDCS is to put all functions required during a whole E-Discovery procedure on the cloud service. This means EDCS enables for E-Discovery participants to collaborate smoothly by removing constraints on working place and minimizing the number of direct contact with target systems. What people who want to use the EDCS need is only a network device for using the Internet. Moreover, EDCS can help to reduce the waste of time and human resources because there is no need to install specific software on every target system and it can give a relatively exact time of completion according to the amount of data for manpower control. Resultingly, EDCS can solve the litigant's cost problem.

Keywords: electronic discovery, E-Discovery, cloud computing, EDRM, IT compliance

1   Introduction

Due to the wide distributions of digital devices like a computer coupled with rapid advances in various IT technologies, Internet has become part of our daily life and the use of the automated information processing system has become more common in every work. Consequently, the use of electronic documents is also rapidly increasing. This situation has had an impact on the judicial system and made all the differences. In litigation, particularly civil litigation in the US Federal Courts, the parties are required, when requested, to produce documents that are potentially relevant to the issues and facts of the matter. This is a part of the process called "discovery". When it involves electronic documents, or more formally, "Electronically Stored Information (ESI)", it is called E-Discovery. Especially nowadays, the growing number of legal cases for civil or criminal trials where critical evidences are stored in digital storages has given the digital forms of information a greater priority as evidence. Moreover, business owners and professional executives are growing more and more interested in E-Discovery since the number of lawsuits is rapidly increasing among business corporations due to conflicts of interest. And also, many global

business firms specially aimed at United States are reconstructing their business processes and deploying the professional e-Discovery service solution to cope with fast-growing IT compliances effectively apart from ERP (Enterprise Resource Planning) solutions [10].

Generally, GRC (Governance, Risk management, and Compliance) is the umbrella term covering an organization's approach across these three areas. Being closely related concerns, governance, risk and compliance activities are increasingly being integrated and aligned to some extent in order to avoid conflicts, wasteful overlaps and gaps. While interpreted differently in various organizations, GRC typically encompasses activities such as corporate governance, enterprise risk management (ERM) and corporate compliance with applicable laws and regulations [9]. Among them, Compliance means conforming with stated requirements. At an organizational level, it is achieved through management processes which identify the applicable requirements (defined for example in laws, regulations, contracts, strategies and policies), assess the state of compliance, assess the risks and potential costs of non-compliance against the projected expenses to achieve compliance, and hence prioritize, fund and initiate any corrective actions deemed necessary. Widespread interest in GRC was sparked by the US Sarbanes-Oxley Act and the need for US listed companies to design and implement suitable governance controls for SOX compliance, but the focus of GRC has since shifted towards adding business value through improving operational decision making and strategic planning. It therefore has relevance beyond the SOX world [12]. Especially since the appearance of SOX, many countries and organizations make their own compliance in recent years, such as HIPAA, GLBA, or SB1386. E-Discovery is also one of the most notable compliances and it is a specialized field for IT. As IT Compliance becomes more diverse like this, all the companies must take a great amount of effort to comply with them and prepare a countermeasure. These factors have resulted in the multiple companies demanding a new type of supporting tool in order to satisfy various requirements of compliance. As a result of that, a large number of E-Discovery technologies related to Digital Forensics have been developed actively and several types of E-Discovery solution have been already released to the market.

The major objective of e-Discovery works is to win a suit. To achieve this goal, the litigants have to secure crucial evidences closely related to litigation issues and apply them to prove their legitimacy. In the E-Discovery procedures, the Potentially Relevant Documents are said to be responsive. The actual conditions or the method of E-Discovery works are performed jointly by both jurists and IT experts who are collaborating with each other. When the litigation is filed, an attorney or a legal team hired by the litigant analyzes the contents of the petition and identifies major issues of the litigation at first. Then, they produce a keyword list about evidences which must be secured on the basis of the litigation issues and deliver it to IT experts. By using the keyword thus generated as well as the specialized tools, IT expert or a special team searches related data for potential evidence and visualizes them for review. After that, attorneys review and analyze again the extracted data from various points of view such as suitability, sensitivity or confidentiality. Finally, all evidences are produced by passing through the procedures mentioned above for a presentation in the trial [1]. Although this procedure sounds easy, it is very complicated works and there are many cases which this procedure is not going well because of several unexpected variables such as system error, data loss.

So, when people do an E-Discovery, there are two important factors that have to be considered obligatorily besides winning a suit. One is a time and the other is a cost. Recently, the volume of electronically stored information that must be considered for relevance continues to grow and continues to present a challenge to the parties. The cost of E-Discovery can easily be in the millions of dollars. According to some commentators, these costs threaten to skew the justice system as the costs can easily exceed the amount at risk. Discovery is a major source of costs in litigation, sometimes accounting for as much as 25% of the total cost. Overwhelmingly, the biggest single cost in E-Discovery is for attorney review time - the time spent considering whether each document is responsive (relevant) or not. Traditionally, each document or email was reviewed by an attorney who decided whether it was responsive or not. As the

volume of material that needs to be considered continues to grow, it is becoming increasingly untenable to pursue that strategy [2]. In addition, according to FRCP(Federal Rules of Civil Procedure) of U.S.A, litigants must submit all evidences within 120 days from the day of lawsuit filed [7]. 120 days seem to be enough time for them to make evidences but the reality is not. Because that period contains a lot of tasks, such as a checking the litigation issues, a discussion about whole e-Discovery schedule or evidence submission format. If litigants can't prepare suitable evidence within the period fixed by law, losing the case is definitely a result. So, attorneys and their clients are looking for ways to minimize the cost and time of E-Discovery.

In order to comply with their request, many E-Discovery vendors have developed and released competitively their own service systems or software applied state-of-the-art technologies and Cloud Computing is one of the most exclusive skills as a computing infrastructure for E-Discovery service. But, this business is still at a preliminary stage. So, a present level is a simple and partial combination between existing E-Discovery technologies and Cloud Computing factors for performance enhancement. On the other hand, there are some solutions which implement all E-Discovery functions based on Cloud Computing through a complete platform conversion. However, these products actually do not cover all E-Discovery works that have to be done and have many drawbacks and considerable limitations [3].

So in this paper, we design a new type of E-Discovery Service Structure based on Cloud Computing called EDCS(E-Discovery Cloud Service) in order to make the best use of its advantages and overcome the limitations of existing E-Discovery solutions. The goal of EDCS is to put all functions required during a whole E-Discovery procedure on the cloud service. This means EDCS enables for E-Discovery participants to collaborate smoothly by removing constraints on working place and minimizing the number of direct contact with target systems. What people who want to use the EDCS need is only a network device for using the Internet. Moreover, EDCS can help to reduce the waste of time and human resources because there is no need to install specific software on every target system and it can give a relatively exact time of completion according to the amount of data for manpower control. Resultingly, EDCS can solve the litigant's cost problem. And then, we introduce a series of use scenario and suggest three implementation methodologies for differentiated functions of EDCS. After analyzing EDCS's practicality, we conclude this paper and introduce our future works finally.

2 Background

2.1 Electronic Discovery

Electronic discovery(or E-Discovery), first introduced by Federal Rules of Civil Procedure amendments on December 1 2006, refers to discovery in civil litigation which deals with information in electronic format also referred to as ESI(Electronically Stored Information) [7]. This is the result that reflects the modern flow that Discovery's main target is ESI. According to these rules, each company has the responsibility to produce their own evidence for winning the suit, and the use of digital forensic tool is almost a necessity.

EDRM is specified legal requirements of E-Discovery mentioned in U.S. FRCP, and EDRM describes the details about tasks of E-Discovery work. This provides guidelines associated to E-Discovery procedure for standardization and describes functional specification of each phase. This guideline can be recognized as a universal standard because it has been developed in consultation with more than 60 leading E-Discovery-related organizations from 2006. Thus, most of the tools and techniques for E-Discovery are designed on the basis of this model [5]. Fig 1 shows EDRM diagram which represents a conceptual view of the E-discovery process.
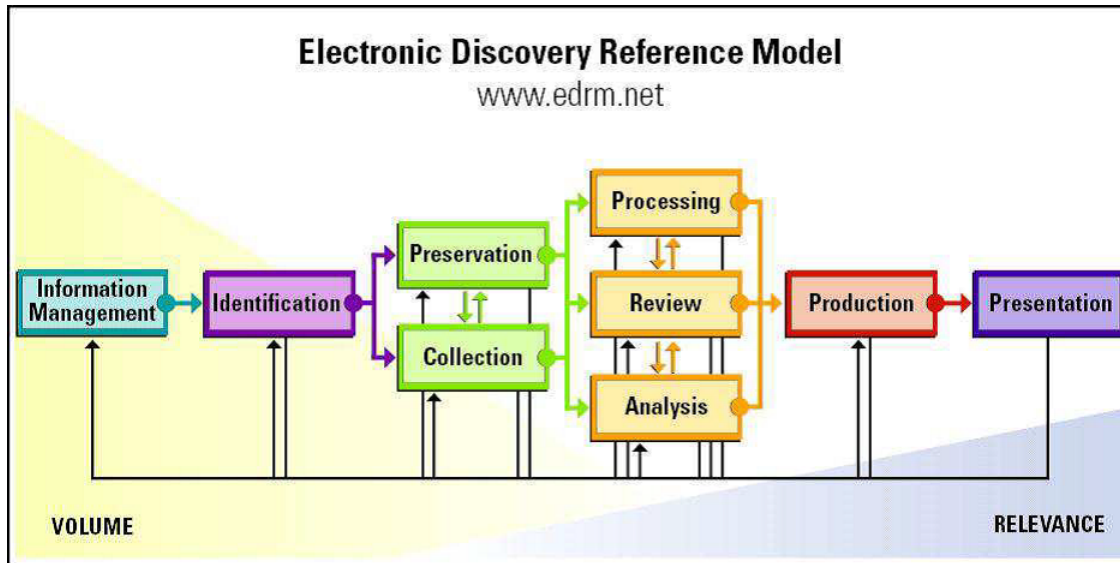
Figure 1: Electronic Discovery Reference Model

2.2 Cloud Computing

A definition of cloud computing by NIST(National Institute of Standards and Technology) [4] is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources(e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing includes various types of services such as: infrastructure as a service(IaaS), where a customer makes use of a service provider's computing, storage or networking infrastructure; platform as a service(PaaS), where a customer leverages the provider's resources to run custom applications; and finally software as a service(SaaS), where customers use software that is run on the providers infrastructure. Cloud computing has the five essential characteristics of cloud computing; rapid elasticity, measured service, on-demand self-service, ubiquitous network access, resource pooling.

Cloud computing structure consists of applications, servers, distributed file systems, distributed databases, caches, and cloud storage, mass data analysis, cluster management, server virtualization, etc. The user connects to the cloud service by using the web browser or the dedicated client, and uses the provided application. Fig 2 shows a simple SaaS structure of cloud computing system.

3 Analysis of Existing E-Discovery Service & Solutions

In this section, we find out major functions, characteristics and limitations of existing E-Discovery service & solutions. Also, we examine the trend of technical development for E-Discovery and identify the practical considerations when the conversion of E-Discovery Service is to be made.

3.1 Major Functions of E-Discovery Service & Solutions

Table 1 shows the phases of e-Discovery and summary from specifications of each phase proposed by EDRM [6].

Most functions of existing E-Discovery Service & Solutions are focused on the following list of five phases(Collection, Processing, Review, Analysis, Production) because all these phases have a high level
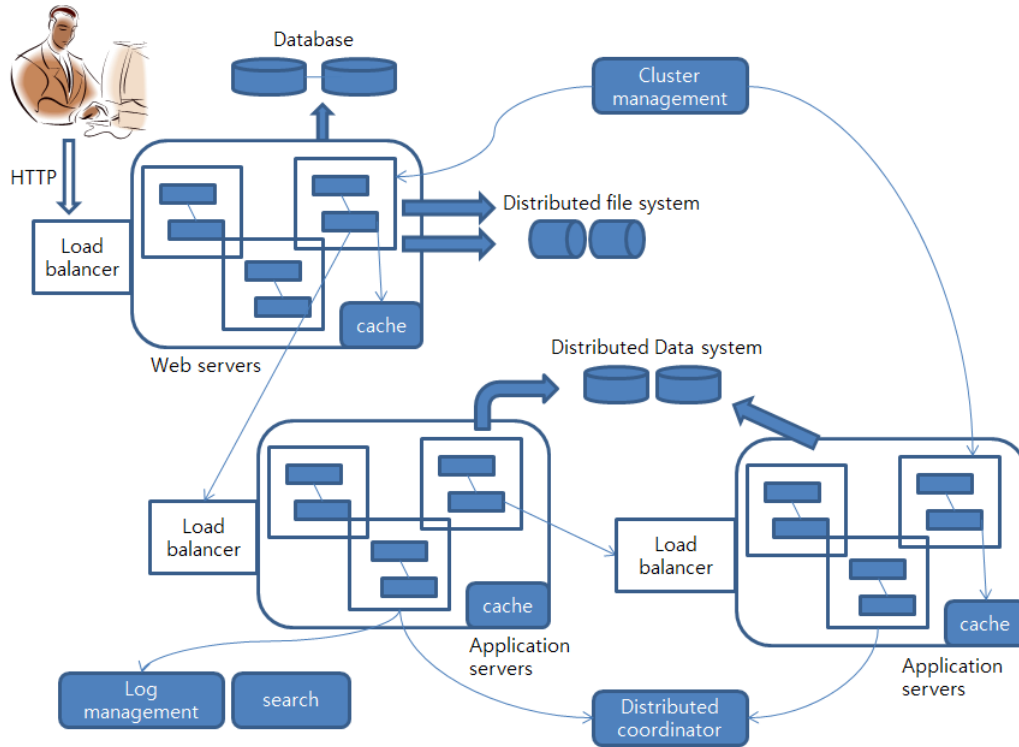
Figure 2: A Simple SaaS Structure of Cloud Computing System

of dependence on tool's performance for efficiency improvement of E-Discovery works [3]. The primary technologies for implementing these tools are as follows.

- Document Indexing & Query Processing for an effective search operation

- Classification for removing of duplicated, patent or confidential documents

- Data Format Converting for using of integrated platform, prearranged evidence production & various format compliances

- Data Visualization for a cooperation of review & analysis operation

- Labeling & Tagging for a document selection based on the relevance with litigation issues

Before attempting to combine E-Discovery Solution with Cloud Computing, most of tools for E-Discovery were developed in a general form called installation type software. It means these kinds of tools must be installed at target system before it is used. So, E-Discovery participants need extra time for software installation beyond total time required for E-Discovery works. In order to reduce time waste like this, pre-installing an E-Discovery tool on every in-house system is time & cost consuming and obviously inefficient. Moreover, installation type software can usually give no guarantee of steady operation pace because operating efficiency of it definitely depends on the performance of system where it was installed.

Table 1: The phases and the summaries from specifications of each phase proposed by EDRM

Phases	Summary of Specifications
Information Management	Phase to manage their own ESI according to organization's information management policy
Identification	Phase to determine scope of e-Discovery target and identify a real ESI for collecting and preserving
Preservation	Phase to protect ESI from a malicious attack or an intentional destruction
Collection	Phase to collect ESI from various types of storages
Processing	Phase to remove overlapping ESI or unrelated data with lawsuit from collected ESIs and convert the ESI to fit the format for an effective review
Review	Phase to sort sensitive ESI according to privilege, confidentiality, privacy
Analysis	Phase to analyze the collected ESI based on Litigation-related information (Litigation issue, Persons, Keyword, Important documents)
Production	Phase to product ESI with a format negotiated in advance
Presentation	Phase to submit ESI an effective way for being crucial evidence

3.2   Convergence of E-Discovery Solutions and Cloud Computing

In recent years, the quantity of a company's data which may become an object of E-Discovery potentially is growing larger day after day and E-Discovery participants are becoming more diverse. Especially, E-Discovery participants may include company's legal team, general employees, staffs, managers in each department, external law firm, or outsourcing company specialized in E-Discovery, etc. They are people who were closely related with litigation, E-Discovery work or litigant parties. So, nothing is more important than smooth cooperation between participants for the success of E-Discovery work.. To reflect this circumstance, the recent trend of technical development for E-Discovery is the convergence of existing services or solutions and Cloud Computing. Fig 3 first introduced in GARTNER 2012 Report shows the famous vendors' position or role in E-Discovery market [3]. This report was compiled based on the investigation of functionality and characteristics of various E-Discovery software and introduce about each vendor's strengths and cautions.

The market covered by this Magic Quadrant contains vendors of e-discovery software solutions for the identification, preservation, collection, processing, review, analysis and production of ESI in support of the common-law discovery process for litigation, regardless of delivery method. Among them, vendor who belongs to the group of leaders and visionaries similarly has a clear intention to develop E-Discovery software based on cloud computing in a form of SaaS although there are some differences between vendors. In general, the convergence is made by a partial phased combination and this kind of E-Discovery service consists of two software parts; one is an installation type which was developed at first to deal with many tasks from Collection to Processing phase and the other is cloud server which was implemented Review & Analysis platform. Using the first software, E-Discovery specialists or hands-on workers can select potentially relevant documents from target system, and convert some document format to suit the integrated Review & Analysis platform and transfer them to cloud server. After that, various E-Discovery participants, especially company's legal team or attorneys in external law firm, can review and analyze a relevance of documents as evidence at the same time with no limitations of place. This is an attempt to reduce wasted cost for review & analysis phase by improving work efficiency because this phase requires a lot of collaboration between various participants. AccessData and Guidance Software are representative vendors who make this kind of product. The reason why they are all belong to the leaders group and choose the way of partial convergence is that they already have a powerful software with similar to the first type and they want to keep using and selling that. However, in the real litigation cases, cooperation
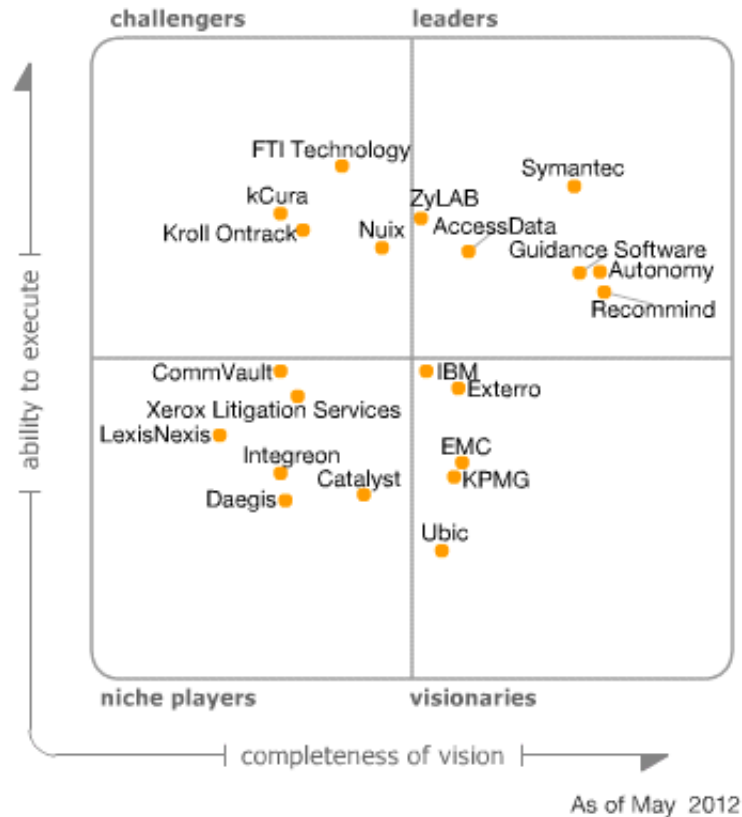
Figure 3: Magic Quadrant for E-Discovery Software

is required through the entire procedure of E-Discovery as well as Review & Analysis. Accordingly, it is necessary to combine additional phases from Identification to Production or to implement all functions on the complete cloud computing platform. At this point, vendors such as Xerox Litigation Service, Integreon are continually trying to develop solution which implements a considerable portion of E-Discovery procedure by using cloud computing technologies. But, they have not produced a noticeable outcome yet and they are classified as the Niche Players Group.

4 Design of EDCS(E-Discovery Cloud Service)

4.1 EDCS Architecture

The goal of EDCS is to put all functions required during a whole E-Discovery procedure on the cloud service. That is, EDCS is serviced in the manner of SaaS. To do this, each function will be implemented in the form of application, and each application will interoperate with separated cloud storages based on its purpose and E-Discovery work schedule. Fig 4 shows the overview of EDCS architecture.

Users of EDCS can be divided into three groups. First group 1 includes E-Discovery target systems which were identified that potentially relevant documents were stored and these systems will be connected for indexing and collection. Second group 2 includes people who have a responsibility to do an E-Discovery works because they were hired as a specialist by a litigant such as attorneys in law firm, staffs in outsourcing company specialized in E-Discovery. Of course, if a litigant is a company and the
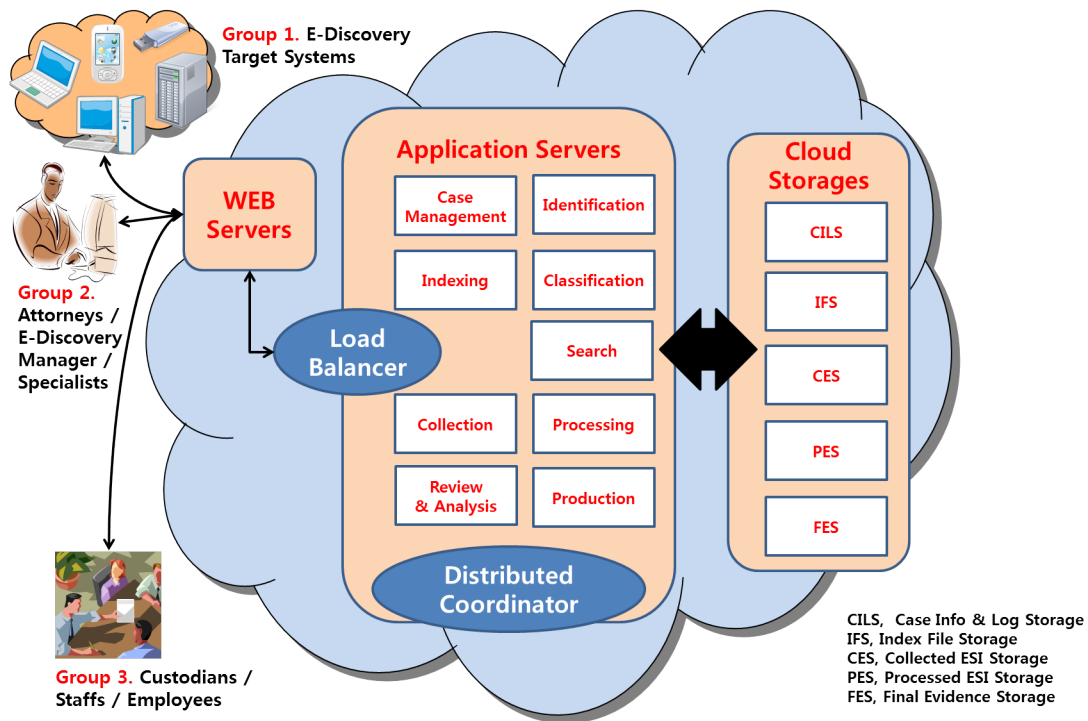
Figure 4: The Overview of EDCS Architecture

company has a legal or E-Discovery team, these people also belong to second group. Last group 3 includes people who are related to the litigation issues and have a duty to interview for Identification.
EDCS consists of 3 parts for the E-Discovery service operation(WEB Servers, Application Servers, Cloud Storages) and 2 parts for the system resource management(Load Balancer, Distributed Coordinator). Blocks depicted in Application Servers section are service applications of EDCS. The name and purpose of each application is shown at next Table 2.

4.2 Use Scenario

In order to use the functions of EDCS, all participants and target systems of E-Discovery have to connect the WEB Servers by using a browser. According to WEB Server's request, Load Balancer assigns an available Application Server and then WEB Server sends a user's request to the Application Server. After that, Application Server executes a specific application corresponding to the use's request. Once the litigation is occurred, the chief of E-Discovery team create a database in CLIS and E-Discovery participants record all the information about the litigation & E-Discovery work by using the Case Management application. People who are involved in the litigation have to connect and give an interview personally according to the procedures of Identification. This can identify E-Discovery target systems, and these systems are indexed by the Indexing application. Using an index, participants can search the potentially relevant documents for the future review of suitability as evidence, and the information produced by a Classification application can be used during this process. Because this application enables to remove duplicated documents and identify sensitive documents which are not supposed to make public such as patent or business secret. Classification result can be saved by updating index files with no extra storage. If target documents for review are decided, Collection application can be used to make a copy of each

Table 2: The name and purpose of each application for EDCS

Name	Target Users	Interoperated Storages	Purpose
Case Management	Group 2	CILS	Saving and managing the all information about case & E-Discovery work(litigation issue, participants, the progress of work, the people concerned, E-Discovery target systems, etc.)
Identification	Group 3	CILS	Providing a specific protocol & reply forms for interview to identify E-Discovery target systems
Indexing	Group 1 & 2	CILS & IFS	Creating index files of each target system for classification & search
Classification	Group 2	IFS	Classifying documents according to contents and updating index files by using the result
Search	Group 2	CILS & IFS	Search for potentially relevant documents related with litigation issue and saving the search result(the path of document)
Collection	Group 1 & 2	CILS & CES	Making a copy of the relevant documents and creating hash values for file integrity
Processing	Group 2	CES & PES	Converting a document file format suitable for integrated Review & Analysis platform
Review & Analysis	Group 2	PES & FES	Providing an integrated platform, visualizing the contents of document, tagging relevant documents as evidence and moving them to FES
Production	Group 2	FES	Convert a document file to the negotiated evidence format and making a final report

original document and save them to the CES. And then, copied files are converted their format suitable for integrated Review & Analysis platform and save them to the PES by using the Processing application.. After all these tasks are completed, attorneys can review and analyze the collected documents and sort out them for the final submission of evidence.. Before the submission, selected documents have to be converted to the negotiated evidence format by using the Production application. In order to increase work efficiency, various participants can progress this whole process at the same time, regardless of sequence. Also, if the participants know that there are unintended mistakes, errors or failings by the evaluation of each application's result, they can go back anytime to the troubled part for reworking.

4.3   Implementation Methods

In order to differentiate EDCS from existing E-Discovery service and solutions, we suggest the following three implementation methods.

- Remote Indexing : The most straightforward method to create index files at the cloud server side is storing all of original documents in the cloud storage. Considering the amount of company's data is rapidly increasing, this method is very inefficient from the perspective of storage efficiency and making backup every day is also inefficient because people can't expect when the E-Discovery work will be needed. Remote Indexing is an alternative to solve these problems. At the beginning, Indexing application of EDCS creates a new user account which is equivalent to the administrator on target system. This function can be implemented in the form of web browser's plug-in. Using

this account, the application makes a reconnection with target system, and start creating index files by using OS dependent functions such as network file sharing or file system mount. Naturally, developers have to prepare additional methods to deal with communication errors for the stability of indexing operation.

- `Classification` : Making a dictionary of terms which were made up documents and vectorizing is required prior to create index files. The function for the automated document classification based on its contents can be implemented by using the information produced through these kinds of operations. To do this, developers can use the machine learning algorithms as the case may be. If the E-Discovery participants can decide categories of documents and prepare appropriate learning samples in advance, supervised-learning algorithms like Support Vector Machine will be useful. Were it otherwise, unsupervised-learning like K-means will be more useful [8]. In addition, using a distributed processing system like Hadoop [11] enables to reduce the entire operation time.

- `Collection` : The function for collection can be implemented in a similar way to Remote Indexing. Using an account created for Remote Indexing, all files in target system can be shared over the networks. The work necessary for collection is only copying files what user want. Above this, hash algorithms can be used to verify the originality & integrity of files. To do this, the application has to get hash values of files before making a copy and compare those values after copy operation.

5   Analysis about Practicality of EDCS

E-Discovery participants can use EDCS anytime anywhere if they have a device for using the Internet. This means there is no need to install specific software on every target system. Especially, the more E-Discovery target systems, the better EDCS is; it can reduce the waste of time & human resources for the software installation. Moreover, it is difficult to get an estimated time of completion in the case of using the installation type software because its operating efficiency definitely depends on the performance of system where it was installed. If the litigant has to hire persons to the number of target systems for the rapid progression of E-Discovery work, it will cost a huge amount of money. On the other hand, EDCS can give a relatively exact time of completion according to the amount of data. This information is very useful for the placement of human resources. For this reason, EDCS can solve the litigant's cost problem. With these advantages, EDCS enables for participants to collaborate smoothly by removing constraints on working place and minimizing the number of direct contact with target systems. Contrarily, there is a consideration about the performance of indexing operation. The biggest influence is the read/write time for the physical storages on the local system indexing, but remote indexing of EDCS is additionally influenced by the communication time. So, it is necessary to verify whether this tradeoff is tolerable through the experiment.

6   Conclusion & Future Works

As IT Compliance becomes more diverse, all the companies must take a great amount of effort to comply with that and prepare a countermeasure. Especially, E-Discovery is also one of the most notable compliances and it is a specialized field for IT. When people do an E-Discovery work, there are two important factors that have to be considered significantly. That is time and cost. These factors have resulted in the multiple companies demanding a new type of E-Discovery supporting tool in order to satisfy various requirements of compliance. As a result of that, a large number of E-Discovery technologies related to Digital Forensics have been developed actively and several types of E-Discovery solution have been already released to the market. However, these products actually do not cover all E-Discovery works

that have to be done and have many drawbacks & considerable limitations. Clearly, the litigant of the future as a potential consumer will constantly demand more useful solution or service. So in this paper, we designed a new type of E-Discovery Service Structure based on Cloud Computing called EDCS in order to make the best use of cloud computing advantages and overcome the limitations of existing E-Discovery service or solutions. And then, we introduced a series of use scenario and suggested three implementation methodologies for differentiated functions of EDCS. Each function was a Remote Indexing, Classification and Collection. Finally, we analyzed the practicality of EDCS and talked about the consideration related to indexing performance. In our future works, we will choose concrete algorithms & development tools and implement EDCS prototype. After that, we will evaluate the substantive performance of EDCS from the various perspective of work efficiency and consistently study on the way of improvement .

References

[1] A. I. Cohen and E. G. Kalbaugh. *ESI Handbook : Sources, Technology and Process*. Aspen Publishers, October 2008.

[2] H. L, Roitblat, A. Kershaw, and P. Oot. Document categorization in legal electronic discovery: Computer classification vs. manual review. *Journal of the American Society for Information Science and Technology*, 61(1):70–80, October 2009.

[3] D. Logan and S. Childs. Magic quadrant for e-discovery software. `http://accessdata.com/gartner-2012`, last viewed May 2012.

[4] P. Mell and T. Grance. The nist definition of cloud computing. `http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf`, NIST Special Publication 800-145, 2011.

[5] T. E. D. R. Model. Edrm framework guides. `http://edrm.net/resources/guides/edrm-framework-guides`, last viewed May 2012.

[6] T. E. D. R. Model. Edrm stages. `http://www.edrm.net/resources/edrm-stages-explained`, last viewed 2009.

[7] T. C. O. T. J. H. O. REPRESENTATIVES. Federal rules of civil procedure. `http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/2010%20Rules/Civil%20Procedure.pdf`, 2010.

[8] F. Sebastiani. Machine learning in automated text categorization. *ACM Computing Surveys*, 34(1):1–47, March 2002.

[9] A. Tarantino. *Compliance Handbook(Technology, Finance, Environmental, and International Guidance and Best Practices)*. John Wiley & Sons Inc., December 2007.

[10] L. Volonino and I. J. Redpath. *e-Discovery For Dummies*. Wiley Publishing, Inc., November 2009.

[11] T. White. *Hadoop: The Definitive Guide 1st Edition*. O'Reilly Media, July 2009.

[12] Wikipedia. Governance, risk management, and compliance. `http://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance#Integrated_governance.2C_risk_and_compliance`, last viewed March 2011.

Taerim Lee received his Bachelor and Master of Engineering degrees from Pukyong National University, Busan Korea in 2008 and 2010, respectively. He is currently doing a Ph.D. program in Department of Information Security, Graduate School, Pukyong National University. His research interests include digital forensics, e-Discovery, cloud computing, and machine learning.

Hun Kim received his B.S. degree in Major of Computer and Multimedia Engineering from Pukyong National University, Busan, Korea in 2012. He is currently pursuing his master's degree in Department of Information Security, Graduate School, Pukyong National University. His research interests include digital forensics, e-Discovery, Cloud System and security.

Kyung-Hyune Rhee received his M.S. and Ph.D. degrees from Korea Advanced Institute of Science and Technology (KAIST), Daejon, Korea in 1985 and 1992, respectively. He worked as a senior researcher in Electronic and Telecommunications Research Institute (ETRI), Daejon, Korea from 1985 to 1993. He also worked as a visiting scholar in the University of Adelaide in Australia, the University of Tokyo in Japan, the University of California at Irvine in USA, and Kyushu University in Japan. He has served as a Chairman of Division of Information and Communication Technology, Colombo Plan Staff College for Technician Education in Manila, the Philippines. He is currently a professor in the Department of IT Convergence and Application Engi-neering, Pukyong National University, Busan, Korea. His research interests center on multimedia security and analysis, key management protocols and mobile ad-hoc and VANET communication security.

Sang Uk Shin received his M.S. and Ph.D. degrees from Pukyong National University, Busan, Korea in 1997 and 2000, respectively. He worked as a senior researcher in Electronics and Tele-communications Research Institute, Daejeon Korea from 2000 to 2003. He is currently an associate professor in Department of IT Convergence and Application Engineering, Pukyong National University. His research interests include digital forensics, e-Discovery, cryptographic protocol, mobile/wireless network security and multimedia content securi-ty.