SecureGov: Secure Data Sharing for Government Services

John (Jong Uk) Choi
Division of Computer Software,
Sangmyung University
Seoul, Korea
juchoi@markany.com

Soon Ae Chun
Columbia University &
City Univ of New York
Staten Island, NY, USA
soon.chun@csi.cuny.edu

Dong Hwa Kim
MarkAny,
Ssanglim Bldg 10F,
151-11 Ssanglim-dong,
Seoul, Korea
dhkim@markny.com

Angelos Keromytis
Columbia University,
1214 Amsterdam Avenue,
New York, NY 10027
angelos@cs.columbia.edu

ABSTRACT

The Open Government initiative allows government data, available digitally, to be shared and integrated to produce value added information products and citizen services. This "paperless" government facilitates the transparency of government and fosters collaboration across government agencies and among citizens. Provision of citizen services often requires sharing citizen data among many different collaborating government agencies, and these data may contain sensitive information of citizens. In this environment, the security and privacy issues become a paramount priority to build a trust-worthy and sustainable smart government. Even though the existing PKI systems can provide secure exchange of information between two organizations, preventing illegal modification, edits, or transfers of sensitive data to third parties for unintended purposes is essential at the end user side. In this paper, we present a framework for secure and trustworthy Government Data Sharing (SecureGov), implemented in the Public Information Sharing Center (PISC) under the Ministry of Public Administration and Security in Korea. The layered security framework uses combined technologies, including a usage control scheme called Enterprise Digital Rights Management (E-DRM) to prevent illegal use and leakage, a forgery prevention technology using a 2-D barcode to prevent illegal modification of the data, and a PKI scheme to ensure the authenticity of the data.

Categories and Subject Descriptors

J.1 [**Computer Applications**]: Administrative Data Processing—*government*; **H.4.m** [**Information Systems**]: Information Systems Applications—*Miscellaneous* **H.3.5.[Online Information Services**]: Data sharing, Web-based Services

General Terms

Management, Design, Security.

Keywords

Security, Privacy, Government Information Sharing, E-DRM, Access control, usage control, forgery prevention, Public records, Citizen Data, Smart Government.

dg.o 2013, Jun 17-20 2013, Quebec City, QC, Canada
ACM 978-1-4503-2057-3/13/06.

1. INTRODUCTION

Open government initiatives encourage governments to share government information for creating a collaborative environment and promoting innovation for further creating better services for citizens and society that would not be possible otherwise, leading to a transformation of government into a so-called "smart government." The first and foremost task for the smart government, thus, is sharing government data with citizens (we will call this G2C sharing). Governments collect numerous data items, including demographic, property ownership, crime, business, intelligence and traffic data, etc. Sharing these government-collected data in an unprecedented manner may create innovative products and services for citizens, businesses and governments. In addition, social media tools generate large amounts of records of citizen voices and opinions about government policies and (in)actions. Thus, the second ingredient of smart government should be openness to receive citizens input data and share them among government agencies in a timely manner to reflect the citizens' feedback about policies and public services (C2G sharing). In addition, the explosion of mobile devices allows citizens to demand more agile and fully context aware government services. Thus, the third key point of smart government is that the citizen-related data collected for public services also should be efficiently shared among government organizations to create more integrated personalized services that can be delivered to citizens anywhere, anytime to any device, transcending space, time and device differences (G2G sharing).

For smart government to be sustainable in these different types of information sharing environments, providing secure and trusted information sharing is one of the most urgent issues, to prevent leakage of secret and sensitive information.

In this paper, we present a security framework for citizen data sharing for Government services (SecureGov) that enables secure sharing of citizens' documents and data among government agencies while delivering citizen services. The SecureGov framework is based on the Service Oriented Architecture with security layers with PKI infrastructure, access control technology, and forgery prevention technology to protect the documents and data from alterations or leakage in transit as well as unauthorized access,modification or disseminations at the client devices. This approach was implemented in the 'Public Information Sharing Center (PISC)' in Korea. We provided this technology solution for SecureGov for PISC to achieve secure delivery and secure use of the citizen data.

The paper is organized as follows: In section 2, we present related work on security solutions in government information

sharing environments. Section 3 describes the Public Information Sharing Center in Korea, and provides a use case for citizens' data sharing in government service processing. In Section 4, we present the government information sharing system (GISS) architecture and components. In Section 5, the security framework, called SecureGov, is proposed to achieve secure sharing of citizen data for governments. SecureGov focuses on end-user usage control for secure sharing. The security components and their functionalities are followed by discussion and conclusions in Section 6.

2. RELATED WORK

To provide security for seamless sharing and interoperability of citizen-service-related information among diverse government organizations, various schemes, such as Public Key Infrastructure (PKI) systems [4, 16, 6], have been suggested. Headayetullah, and Pradhan [7][16] provide data integrity using the MD5 encryption algorithm, confidentiality and authentication using PKI and agency identity verification using a mapping function in information sharing at government organizations. However, the MD5 encryption scheme is considered cryptographically broken, and the NIST recommends US government applications to use SHA-2 or SHA-3 hash functions [18]. Nortel, Casey, Harbitter, Leary, and Martin [3] propose a framework for secure information sharing, emphasizing the importance of encryption, PKI, multi-factor authentication, federated ID management, role-based access control, etc. Liu and Cheta [12] suggested an Internet-based trust model architecture for information sharing among government organizations. In their research, trust is considered important, while negotiation is more important than other factors. Makedon, Sudborough, Baiter, Pantzion, and Conalis-Kontos [13] concluded that fear of revealing sources and losing autonomy may result in costly and redundant efforts that lower productivity and achieve only limited data-reuse and integration. They propose a negotiation-based information sharing system that includes effective rewards and ensures due credit.

Park and Sandhu present $UCON_{ABC}$, a usage control model that recognizes ongoing control for relatively long-lived access or for immediate revocation [27]. Sandhu, Ranganathan, and Zhang [16] provide Trusted Computing (TC) technologies that can facilitate secure information sharing such that the shared object can be protected and viewed only by a Trusted Viewer (TV). They developed the PEI framework of Policy, Enforcement and Implementation models to protect the shared information. Specifically, the three layer trust model includes policy-level issues such as revocation policy, usage policy, re-dissemination, distribution and accessibility policies, while the enforcement layer considers the password-based, device-based and credential-based enforcement models with encryption technologies for shared object protection. However, their research makes a simplifying assumption for the PEI framework to handle exclusively read-only information with TV. Thus, mechanisms to protect editing or modifications or to enforce other policy level security policies such as usage or distribution control at the end user (client-side) are not provided.

Even though the above PKI scheme-based security mechanisms can provide authentication, confidentiality, and non-repudiation for shared information between government organizations, there still remain several problems and potential risks. PKI can guarantee secure delivery of documents between authorized parties and block illegal modification while a document is in transit. However, even if the document is delivered to the right party without any modification, it can be illegally modified at the recipient's devices after delivery, or its content on the screen can be easily copied into a new file and disseminated for sharing with third parties without proper authorization. For example, a document containing criminal records is delivered to person B at organization-B from organization-A. The document is decoded using symmetric key encryption between organization-A and organization-B and then it can be opened at B's computer. Using the functions 'cut and paste' and 'screen capture,' the document can be easily copied into a new file and modified. That means that PKI provides secure delivery of a document between two parties or multiple parties, but cannot guarantee secure 'use' of the document, protecting the sender from misuse after it is delivered.

In this paper, we present the secure data sharing framework for government services (SecureGov) that can provide the security of content in transit as well as protect the content at the end-user devices, extending the usage control capabilities in DRM systems.

3. BACKGROUND

3.1 Public information sharing center (PISC)

Korea initiated the Public Information Sharing Center (PISC) in 2005 through a steering committee, and officially launched it in 2010 as a center under the Ministry of Public Administration and Security (MOPAS) [19]. MOPAS is part of the Korean central government, established in 2008 by integrating the Ministry of Government Administration and Home Affairs, the Civil Service Commission, the National Emergency Planning Commission and national information management strategy functions of the Ministry of Information and Communication. MOPAS handles national administration, government organizations, personnel management, e-government and disaster safety, and supports the local governments in their administration, finance, and regional development allowing for a great degree of local autonomy.

MOPAS has been in charge of developing e-government policies and implementing services. The ministry spearheads efforts to establish and revise policies and systems to increase the efficiency and productivity of the public administrations and citizen services. It plans and implements organizational restructuring, consolidates collaboration systems among different central government organizations and promotes private sector involvement in government affairs.

MOPAS has launched Korea's e-government portal for Online Public Services (called Minwon24) where 24-hour online services are provided to any citizen, anytime, anywhere. The online services enable government officials to search and look-up of citizens' registered information and allow citizens to submit applications for issuance of civil affairs documents certified by appropriate government agencies without having to visit administrative offices. Some of these citizen services include resident registration, education access and vehicle registrations. The ministry also leads smart-government efforts, including smart citizen services, by sharing among government agencies the real-time reports of citizens complaints (e.g., damaged roads) with photographs taken from smart phones; smart security by utilizing CCTV photographs to investigate violent crimes and missing children; and smart disaster management by real-time monitoring of natural disasters such as floods and landslides.

In the process of Internet-based citizen records processing services at local governments, the audit commissions pointed out the risks that citizens' records might be modified, forged or leaked. To address the problem of security and privacy in citizens'

records processing, the Public Information Sharing Steering Committee was established and spearheaded constructing the secure government information sharing system for citizen records services [20].

3.2 Sharing Environment for Public Records Services

Issuing a certified government document based on public records at the request of a citizen might require cooperation from many government organizations, and appropriate information or supporting documents should be available to verify and cross-check the authenticity of data before issuing an official document. These supporting documents often reside in different agencies or organizations, thus citizens need to prepare them beforehand as part of a public records application package.

One example of public records services can be illustrated bythe issuance of a passport. In Korea, passport applications are submitted at local government offices, but the passport records and application processing are collectively managed and controlled by the Ministry of Foreign Affairs (MOFA). In issuing a passport, several citizen data sources need to be checked, such as family registry records managed by a local government office, military service records managed by the Office of Manpower Service, driver's license information managed by the National Police Agency, and others. As depicted in Fig.1, some data should be forwarded to other organizations for verification or certification, and others are collected from relevant agencies to process the application for passport issuance. Before government information sharing, citizens who applied for a passport had to visit many different government offices to collect certificates and supporting documents.

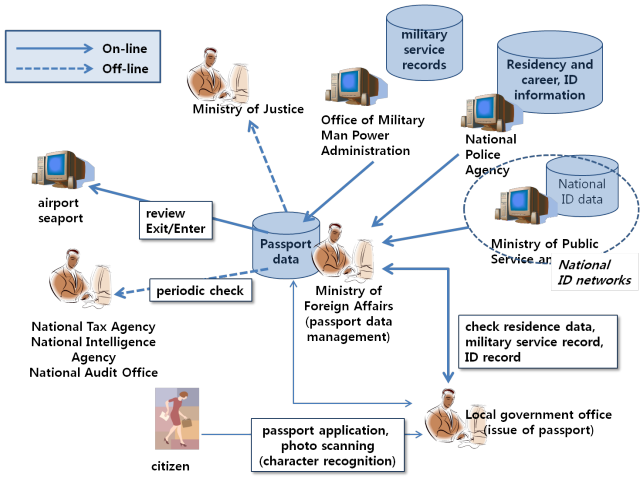

Figure 1 Government Information Sharing for Passport Service

Likewise, when a citizen applies for government welfare support, which is provided to low income households at a local government office, citizens need to provide records and documents from other local government offices, the National Tax Agency, the Ministry of Public Service and Security, and four major social security insurances organizations (NP: national pension, HI: health insurance, EI: employment insurance, WCI: worker's compensation insurance). Because of multiple bureaucratic checks inherent in the Korean public service system, there has been a high demand for 'government information sharing.'

4. GOVERNMENT INFORMATION SHARING SYSTEM

PISC has developed a government information sharing system (GISS), which facilitates the exchange and sharing of citizen data among government agencies and some public and private organizations to provide better citizen services. For instance, passport applicants can submit the passport application and take a photo by visiting a local government agency once. The application is registered in GISS, along with the photo, and the citizen request is forwarded to the appropriate agency (in this case the passport processing agency), and the application is digitally accessed by that agency, along with all the accompanying documents. All other relevant records required for verification or processing of the application can be accessed through sharing services in GISS, through information requests to other agencies. The responsible government officer can easily look up all records residing in different organizations through the GISS lookup service at his own computer to process the citizen's application. In addition, online application submissions for several services are possible directly through the citizen service portal (called Minwon24) using the citizen's own device.

GISS lifts the burden of visiting different government offices to prepare necessary documents, saves the costs of collecting and storing duplicate citizen records in different government offices that may cause data integrity and redundant storage issues as well as a heightened risk of leaking sensitive information. In addition, GISS lowers the risk of forgery and illegal modifications associated with paper-based documents.

Since the launch of the GISS in 2006, the number of shared information types has increased from 34 to 120 and is estimated to be 135 in 2012, thus, eliminating the burden of attaching separate documents by citizens [21]. The major categories of shared information include residency-related records, patent or other, legal records, welfare/education/special needs records, property and tax-related records, business-related records, vehicle records, employment license and health license records, and many others. Each category has numerous other subcategories of citizens' information required for certification and verification documents in various citizen requests.

The participating organizations also grew from five public service organizations to 106 public organizations, 18 financial institutions, and 18 educational organizations along with all government administration agencies [21]. Table 1 shows the statistics over the three years from 2009 to October 2012, including the number of annual GISS usage cases that grew to almost 142 million cases, the cost savings in million dollars each year, and the carbon reduction in tons, acheived by sharing the digital records and by avoiding the paper- based documents.

Table 1 Statistics of GISS Usage and Cost Savings (source [21])

Year	# of cases	Savings ($M)	CO2 Reduction (t)
2009	61,249,124	215.5	122
2010	17,641,175	239.2	133
2011	28,592,621	369.4	212
2012	34,325,980	433.3	249
Total	**141,808,900**	**1,257**	**716**

The GISS architecture is based on the Service Oriented Architecture (SOA), with distributed systems from different

participating government agencies and other institutions. The SOA-based architecture for GISS is shown in Figure 2. The SOA architecture enables the distributed and heterogeneous systems of different organizations to exchange and share information through middleware brokerage services provided by GISS without modifying each agency's existing application systems. The SOA framework is popular for developing a sharing environment between disparate systems used by many organizations, as in incident or crisis management systems. Shafiq et al. demonstrated the Department Homeland Security SOA middleware framework, called UICDS, to enable sharing of resources required for incident management [22]. The key idea is that one agency can request a service (e.g. an information lookup service) and the service request is mediated through the GISS middleware broker to identify the service provider agency, and to forward the requested service to the provider agency. Upon receipt of the request notification, the provider agency can access the requested service information, process the requested item and return it through the GISS brokerage, which will forward it to the original requesting agency.

The SOA architecture does not require a centralized data warehouse or database system that contains all data from different agencies in a centralized system with a uniform data schema. The integrated database approach is costly and can pose a greater risk of data loss and sensitive data leaks, in cases of central database attacks. The database approach is also not popular, since it can engender resistance from different organizations that do not want to participate, since they need to give up the agency specific datasets, which amounts to a loss of autonomy as well as increased data latency issues.

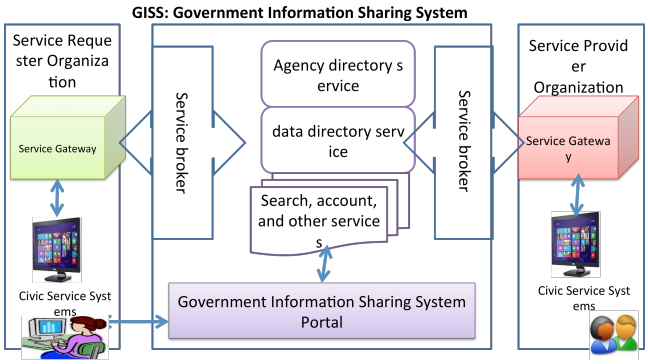

Figure 2 SOA-based Architecture for Government Information Sharing System

Even though government information sharing has been recognized as an essential ingredient for providing seamless government services, and the design of the GISS architecture was completed much earlier, the implementation of GISS had been delayed until the late 2000s, because of security and privacy concerns such as sensitive information leakage and unauthorized modifications. Earlier digital government projects had employed PKI encryption mechanisms that provide secure delivery of information between government organizations. The powerful mechanism of user authentication and confidentiality of PKI systems can assure that the information can be securely delivered to the right person through a controlled process. However, PKI cannot guarantee that the information delivered to the end-user will not be copied and sent to malicious users, or be modified and forwarded to others for financial gain.

The Public Information Sharing Center (PISC) came to recognize the importance of security mechanisms at the end-user sites in addition to the PKI scheme to prevent information leakage and forgery. In the following, we present the security and privacy framework used to establish the secure Government Information Sharing System (SecureGov). SecureGov employs E-DRM (Enterprise Digital Rights Management) to control end user's access to and usage of the citizen data and a 2D-Barcode mechanism to prevent forgery.

5. SECURITY FRAMEWORK FOR GOVERNMENT INFORMATION SHARING

5.1 Security Components for SecureGov

The framework for secure citizen data exchange and sharing for government services (SecureGov) has several security mechanisms, aiming at the access and usage control at the end user (service requester/client) side. The components consist of (1) a PKI component that generates the public key certificates to authenticate the service requester identity, (2) a DRM server component that verifies the roles of the requester, checks the rights and generates the document rights container (e-Container); (3) a DRM-packager component that encrypts the document at the service provider (document source organization); and finally, (4) an E-DRM client component at the requester side that enforces the rights and controls the permissible manipulation of the received documents.

Figure 3 shows the SecureGov security components and data flow of the secure government information sharing system at PISC. When a user of GISS (a government official processing a citizen's application) needs a document that is available in a different organization, he sends a request and PKI certificates to the GISS Server using a Web application form. Upon the submission of the Web-based application, the e-container that includes the request information is automatically generated. The e-container includes detailed information, such as the requested document, the purpose, the requester, his/her department or organization, the requested operations ('read', 'print'), and the expiration date. Currently, two operations are possible, namely 'read,' and 'print' documents at a requester's device. The e-container at GISS is forwarded to the DRM server where the validity of the request is checked by retrieving government-stored employee (requester) information from the proper database. Based on the credentials such as role or position, department, and job assignment, the DRM server creates an 'E-DRM rights' sub-package and includes it in the e-container.

In the next step of processing, the e-container with E-DRM rights is delivered to the destination organization (service provider) where the requested document resides. After the service provider system finishes review of the request package, the document requested is encrypted with the E-DRM rights by the DRM-package module and the encrypted document is sent to the requester through the GISS Internet delivery service.

When the encrypted documents arrive at the device of the requester, the E-DRM client module that resides at the requester client device enforces the access rights and controls the requester's interactions with the documents, according to the E-DRM access rights information encoded with the documents. For example, when the requesting official does not have an access right 'to print document,' but tries to print it using a network printer or virtual printer, printing is blocked. In an extreme case, the document is immediately erased from the applicant's terminal or device.

In summary, the security framework for SecureGov relies on the combination of multiple security mechanisms. The PKI manages and controls the secure delivery of the e-container from the requesting official to a document provider organization, and the delivery of the document from the provider organization to the requesting organization's official. The DRM server component in the GISS verifies the credentials of the requester and issues E-DRM rights to be used in controlling the interactions with the requested document. The PKI is also used in encrypting the document and the E-DRM rights. When the encrypted document with E-DRM rights is safely delivered to the requesting official, the E-DRM client module manages and controls the access and usage rights to the document. It also provides other end-user security mechanisms such as watermarking and a forgery prevention mechanism we will present in Sections 5.4 and 5.5 respectively. In the following subsections, we present more details of the security modules for SecureGov.

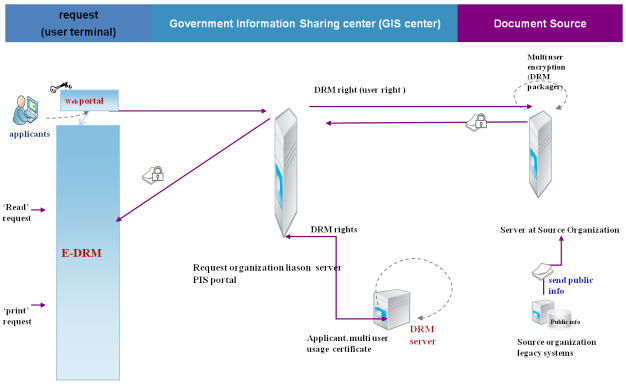

Figure 3 Security Components in Government Information Sharing System

5.2 E-DRM for End-User Access Control

E-DRM was derived from DRM (Digital Rights Management) technology, which was developed to deliver digital contents and to prevent illegal copies and distribution of the digital contents [1][5]. DRM technology's copyright protection capabilities primarily rely on data encryption and access control functions. In general, encrypted contents such as songs or movies are delivered to a user with an encryption key which may be in the same content package, or sent through a separate channel. At the authorized recipient's terminal or device, the contents are decrypted and played. Because the documents are encrypted with a key delivered to the user, when they are illegally copied and sent to unauthorized users, they cannot be properly played. A DRM agent decrypts packaged contents and enforces access control to the contents based on the payment conditions, such as the number of plays allowed, whether to be able to send the contents to a third party, etc. Currently, the access control of DRM systems in playing digital contents is very simple: 'play' or 'don't play.'

E-DRM technology was developed to prevent the illegal leakage of enterprise assets within an intranet environment, while the DRM technology was developed to protect the copyrights of digital contents in the Internet environment. E-DRM relies on encryption and access control for end-user operations as in traditional DRM. Because the documents in E-DRM are encrypted, they are protected from illegal leakage. For example, some users download a file from an enterprise document shelve and make an unauthorized copy on a USB stick or a CD, and then take it outside of the physical boundaries of the enterprise. Even though the documents are encrypted and cannot be opened in a readable state, the end user can make illegal copies. In other words, the strong encryption function of E-DRM technology is powerful in preventing information leakage (i.e., provides content protection), but it does not provide the range of access control functions necessary to limit the end user's activities (i.e., usage control).

E-DRM is quite different from the traditional DRM technology in that more activities on a user's end are controlled. The end-user activities controllable by the E-DRM agent are much wider, to support business requirements, such as 'read,' 'save,' 'edit,' 'print,' 'expiry date,' 'cut and paste,' and 'screen capture,' while the access control functions of DRM are frequently limited to 'play' of the contents.

Generally, an access control specification of E-DRM is epxressed by three parameters: user (who), object (which), and operation (what). First, the users of E-DRM are categorized by position or role, department, and job assignment. Secondly, the object refers to data or documents that can be categorized into security classes such as 'highly confidential,' 'confidential,' 'limited,' 'public,' 'limited to accounting department,' 'limited to R&D department,' etc. (Note that this goes beyond the standard classes of Top Secret, Secret, Classified, and Unclassified). Finally, operations are access rights to objects and are categorized into 'read,' 'save,' 'edit,' 'print,' 'expiry date,' 'cut and paste,' 'screen capture,' and others. Therefore, based on the access control triple, E-DRM evaluates and enforces the access control policies for the shared documents or data.

For example, in Figure 4, let's assume that user A sends a document to several users in the intranet, e.g. user B (Director of Accounting department), user C (Manager of IT department), and user D (Intern as secretary to Director, Production department). Their access rights are managed by the intranet. The user B, as Director of the Accounting department, is given full rights, thus can 'read,' 'save on the local hard drive,' 'edit using cut and paste functions,' 'print three times,' 'keep the file for three days', and then can 'forward to a third party.' However, the user C who is Manager in the IT department can 'read,' 'save on his/her local hard drive,' 'edit,' 'keep the file for three days,' but cannot 'print.' The user D, as an intern, is given limited rights to use the documents only 'to read,' but cannot do anything else. Assume that the user A tries to make a copy of the file on his/her own computer and send it to user F who is not registered in an E-DRM systems directory. In this case, the user F who cannot authenticate himself and has no rights cannot even 'read the file,' because it is properly encrypted. Certainly, he cannot do anything else with the documents.

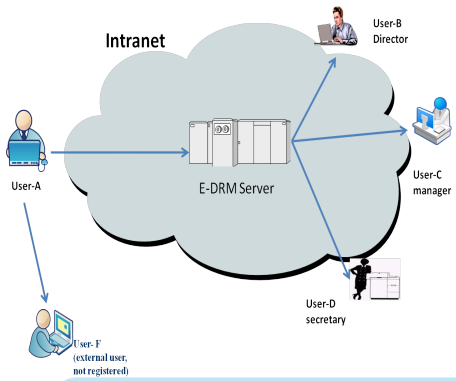

Figure 4 Access Control of each user in a Network

5.3 DRM-Server and DRM-Packager

As discussed in the previous section, the requested information is automatically packaged into an e-container with PKI certificates, and then delivered to the GISS server from a requester to a document source/provider organization. The DRM server in GISS checks the request and decides whether the requested access right is properly

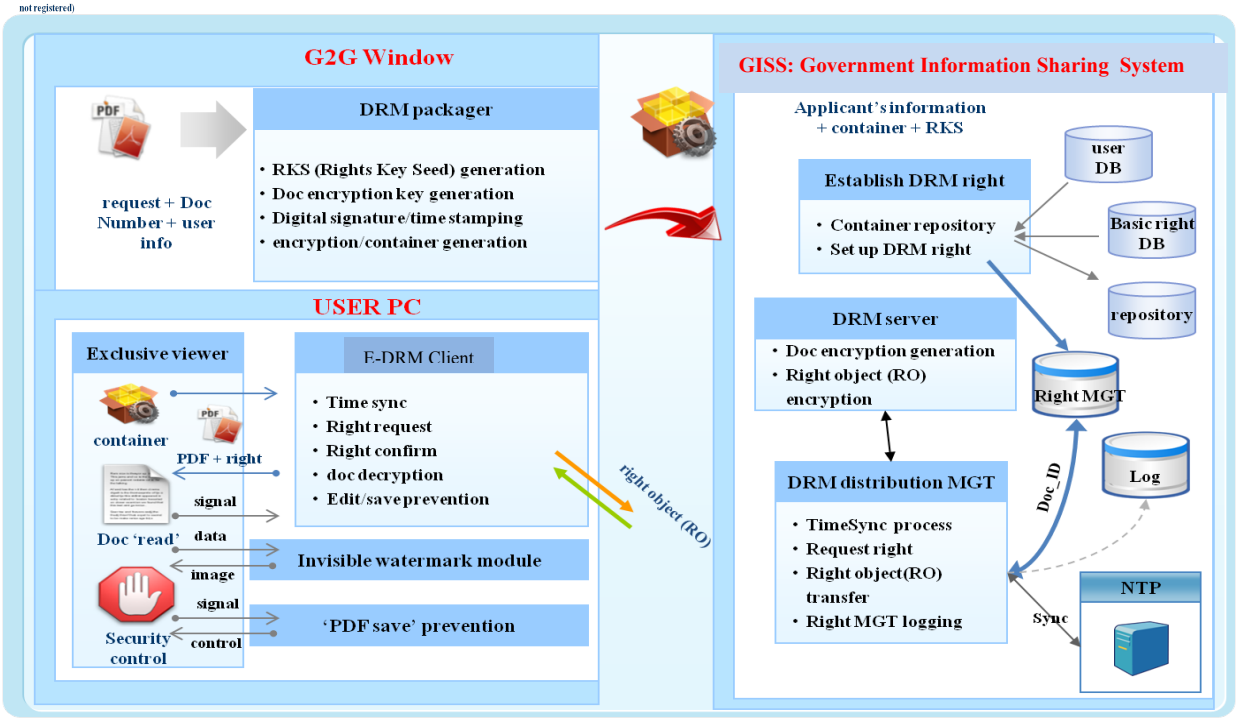

Figure 5 SecureGov Components and Process: DRM Server and E-DRM client

specified or not. The human resources database in the GISS server provides information about the requester, such as her position, department, assigned job, and times of service. Based on the requester's credentials, the DRM-server generates an access control list (ACL) and attaches the list to the document in the e-container, which is then sent to the destination organization to retrieve the requested information ordocuments.

The retrieved document and ACL in the e-container is encrypted by the DRM-packager module at the data providing organization. The encrypted document with E-DRM access control is sent to the DRM distribution management unit in the GISS server that delivers it to the requesting organization end user. This process is very similar to the job of a Right Object server in traditional DRM systems, which creates an of access control list for a user, and then encrypts the requested digital contents before transferring control to a DRM agent on the client's end. In this stage, a time stamp is used to prevent possible disputes over the authenticity of the request and feedback.

5.4 Other Security Mechanisms for End-User control

When a document arrives at the requester's computer, PC or mobile device, it is decrypted first, and then controlled by the E-DRM agent. Because the e-container is encrypted with a user's public key and delivered to the requester, the package can be decrypted only by the private key of the authorized recipient. When the end user (requester) successfully decrypts the message to open the package, he/she can use it according to the predefined access rights. If the user who receives the document package is not eligible for the e-container, he/she cannot open the package in a normal way without the private key and thus cannot read the documents. Even if the user opens the documents, if s/he does not have the privilege of 'save on the user device,' he/she cannot save the document on the hard-drive or mobile device. Also, if the user does not have a right to 'edit,' he/she cannot edit the document. The control of the 'print' function can be enforced in the same way as of the other functions, 'save,' 'read,' and 'edit.'

The screen capture function at a user PC can be deactivated when the user does not have the right of 'screen capture.' As there are so many available capture programs on Internet sites, users can create a new file by capturing each page of the decrypted documents and by editing them into a file. However, the screen capture function is completely blocked by the E-DRM agent and thus it is not possible to capture the content on the screen.

Under the current GISS implementation, only limited eligible end-users have the right to print a document, since the printed documents can be easily scanned to generate a new electronic copy of the document, which can be easily disseminated or shared with unauthorized users. For this reason, only high level employees are allowed to print in the government. However, there is still a possibility that a user with the print privilege can duplicate the printed document by scanning it. To prevent this, GISS automatically embeds invisible watermarks into the printed document, which hide multiple items of information in the visible watermark. Information of the person who printed the document, and also 'which printer was used,' 'which network port was used,' 'when was it printed,' etc. This invisible watermark is a very useful tool in deterring illegal photocopying of printed documents and transferring confidential information to a third party, since one user can be identified as the source of the illegal duplication and dissemination.

For example, in a meeting of eight members each of which printed her/his copy of a document, each copy has invisible watermarks embedded into a printed company logo. If a copy of the document is illegally sent to a third party or competitor, the information hidden inside the printed logo can be used to determine who has leaked the document. As each document carries different information, even though they look exactly the same, the logo can be used in tracing back who leaked the document.

5.5 Forgery Prevention Technology

In implementing a paperless government, one of the most serious concerns is forgery. Because data and documents are digital, there are many ways in which they can be created, modified, and manipulated with simple operations. Especially, as many authoring tools are available on the Internet, the digital document delivered to a requesting official can be easily modified and forged. This is a serious threat against the authenticity of government certificates and documents such as notarized documents that carry legal impact and thus need to be trustworthy.

An effective forgery prevention technology has been employed in certificate printing in Korea for the past 10 years. Many government issued certificates can be printed at home or at work, using standard printers. In order to prevent illegal modifications of the certificates, a 2-D barcode such as shown in Figure 6 is used that contains data from the certificates such as the format information and data content. The 2-D barcode of the certificates is generated by the following conversion procedure. Firstly, the contents of the certificates with format information are collected for conversion. Secondly, a hash value is generated from the content data. Lastly, the content data and hash value are encrypted and converted into a 2-D high density barcode. An error-correction code (ECC) is included in the conversion process. This 2-D barcode can compress 442 bytes into an area of 1 by 2cm. One of the advantages of this 2-D barcode is that any file format can be used in this scheme, including XML, HTML, Tiff Image, and others.

This 2-D barcode can be extended by adding cells. Because an error correcting code is used inside the 2-D barcode, even if 40% of the barcode is lost, 100% of recovery of the original contents is still possible. The 2-D barcode algorithm has not been disclosed, but a verification tool can be provided to rightful users to authenticate a document.

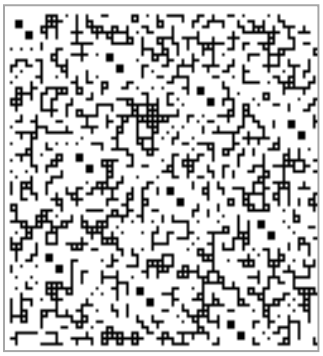

Figure 6 2-D Barcode as End-user forgery prevention

6. CONCLUSION & FUTURE WORK

In this paper, we presented the Government Information Sharing System (GISS) implemented by the Public Administration Information Sharing Center in Korea. GISS facilitates sharing of citizens' records among different government, public, educational and financial organizations to serve citizens with government issued document services. GISS is implemented with the Service Oriented Architecture between the service requester and service provider organizations through the use of middleware brokerage services. The security issues in GISS arise whenever the shared documents should be delivered securely and accessed and used appropriately by the end user (the data-requesting official). To provide the necessary security in the GISS, we presented SecureGov, which is the security framework and implementation for secure sharing of citizen data for delivering government services. The security mechanisms used in SecureGov include: the PKI encryption system to ensure document integrity in transit and user authentication; the DRM-server and the DRM-packager that verify the end-user access capabilities and encrypt the end-user access control information for the shared document; the E-DRM client component that enforces the access and usage control for end-user manipulations of the data and documents. In addition to these, we presented end user control mechanisms, such as the watermarking and 2-D barcode insertion, to prevent illegal leakage of data or to detect the unauthorized dissemination of documents.

The SecureGov security framework can be usefully implemented by any government in any country. The US government had to abandon a three year effort to establish a central data-sharing system with a centralized cross-government citizen database [25][26], which would allow all government departments to share the personal records of citizens in the country. The failure can be attributed to many factors, such as the complexity of linking diverse systems in many agencies, as well as to the costs. The failed system design resorted to a centralized data warehouse. The data from other government entities had to be transferred and stored in the data warehouse. On the other hand, our GISS approach uses the distributed Service Oriented Architecture, where data remains at its source, but is delivered when a request is made. In addition, the security risk of civil servants snooping on personal data were a big issue, which was not adequately addressed. Our SecureGov approach

can be utilized for this kind of endeavor with the emphasis on end-user access and usage control of the citizen data.

There are still many challenges to be solved in order to achieve secure and smart government document sharing. The current study focuses on the G2G sharing environment, where the citizen data or documents are exchanged and shared by the government agencies for their administrative processes. The on-going work extends the secure sharing of government information to a *smart sharing* (SmartShare) environment, where the government shares information with the citizens or businesses (G2C sharing) as in the smart disclosure initiative [23]. In addition, the smart sharing environment should consider cases where the citizen data generated by citizens themselves or collected by businesses (financial, health data) can be directly accessed by and shared with the government (C2G sharing). In this environment, the personal privacy issues become the biggest concerns. Some research proposes how to protect privacy through technologies of data integration and re-use through mashups [24]. However, easier and more frequent access and sharing of personal or business data by and with the governments requires proper security and privacy mechanisms. Our research on a smart sharing environment is ongoing. .

Other technical challenges to be solved when providing public services and information sharing are related to mobile technology and to an extension of legal proof capability. More and more citizens in Korea demand their government services to be delivered to their mobile devices. For example, banking transactions through mobile phones have increased very rapidly. In February 2012, Bank of Korea disclosed that the number of mobile banking transactions increased from 11.2% of all transactions in 2010 to 19.7% in 2011. Registered users at banks increased by 50.6% from 15,750,000 in 2010 to 23,720,000 in 2012. It is especially interesting to observe that the number of smart phone users in the mobile banking sector has increased considerably, to more than 10 million, a 297% increase since 2010. Similar to the explosive growth in mobile banking and e-book downloads, mobile services will increase in the government area. Many government organizations and agencies already provide mobile services, and therefore information sharing through mobile devices might be coming sooner rather than later.

The Korean government also aims at providing a smart work environment for more than 30% of government employees by 2015. Most of the smart work will be realized through mobile systems and devices. Technical issues in the mobile computing era include context awareness and personalization in authentication of users, secure exchange, storage and use of digital documents at mobile devices, prevention of illegal document transfers and possible forgery, and hacking problems in mobile devices.

Legal proof capability of security mechanisms should be further extended in the mobile environment, even if a time stamp and hash value attached to documents are currently sufficient to settle most legal disputes. Because the time stamp and hash value are managed and controlled by GISS itself, there may be concern over legal effectiveness that may have to do with conflict of interest situations.

6. ACKNOWLDEGMENT

This work was conducted while Chun was on sabbatical leave at Columbia University. This work was partially supported by the National Science Foundation DUE1241687.

7. REFERENCES

[1] Arnab, Alapan, and Andrew Hutchison, Requirement Analysis of Enterprise DRM Systems, Proceedings Information Security, South Africa, 2005.

[2] Bajaj, A., Ram, S. IAIS: A Methodology to Enable Inter-Agency Information Sharing in eGovernment, Journal of Database Management, 14, 4, 2003, pp.59-80.

[3] Casey, T., Harbitter, A., Leary, M., and Martin, I. , Secure Information Sharing for the US Government, White Papers, Nortel Technical Journal, 2008.

[4] Chongthammakun, R., and Jackson, S.J. Boundary Objects, Agents, and Organizations: Lessons from E-Document Systems Development in Thailand, Proceedings of 2012 45th Hawaii International Conference on Systems Sciences, 2012.

[5] Elisabeth, H. How enterprise DRM works: Everything you need to know about information rights management, Computer World, 27 April 10, 2010.

[6] Fokoue A.,, Srivatsa, M., Rohatgi, P., Wrobel, P., and Yesberg, J., "A Decision Support System for Secure Information Sharing", Proceedings of the 14th ACM Symposium on Access Control Models and Technologies, 2009: 105-114.

[7] Headayetullah, M., and Pradhan, G.K. Interoperability, Trust based Information Sharing Protocol and Security: Digital Government Key Issue, International Journal of Computer Science and Information Technology, Vol 2 (3) June 2010.

[8] Jang YH, Jungwook Moon, Sam Youl Lee, MyungJae Moon, and TaeJoon Na, Analysis of structural and Practical Factors, related to Information Planning at Public Service, research report, Research Institute of IT and Communication Policy, June 02 2005.

[9] Kido, H. e-Government for Management, Interface, Accountability, and Transparency: Reform of Public Management through ICT", Proceedings of Korea Association of Public Administration, October 18-19, 2002.

[10] Kim, S.W. "A Study on the Public Administrative Information Sharing Scheme for Sustainable Evolution of e-Government", Industry and Management, Chung-book University, 21, 2, 2009, 59-79.

[11] Legner, C., and Lebreton, B., Business Interoperability Research: Present Achievements and Upcoming Challenges, Electronic Markets, Vol.17, No.3, 2007: pp.176-186.

[12] Liu, P., and Cheta, A., Trust-based Secure Information Sharing Between Federal Government Agencies, Journal of the American Society for Information Science and Technologies, 46, 3, 2005: 283-298.

[13] Makedon, F., Sudborough, C., Baiter, B. B., Pantzion, G., and Conalis-Kontos, M., A Safe Information Sharing Framework for e-Government Communications, IT white paper from Boston University, 2003.

[14] Otjacques, B., Hitzelberger, P., and Feltz, F. Interoperability of e-government information systems: Issues of Identification and Data Sharing, Journal of Management Information Systems, Vol.23, No.4, 2007: pp.29-51.

[15] Pardo, T. A., Gil-Garcis, J.R., and Burke, G.B. Building Response Capacity through Cross-boundary Information Sharing: The Critical Role of Trust, Proceedings of E-Challenges Conference, 2006.

[16] Sandhu, R., Ranganathan, K., and Zhang, X., Secure Information Sharing enabled by Trusted Computing and PEI models, Proceedings of the ACM Symposium on Information, Computer, and Communication Security, 2006: pp.2-12.

[17] Headayetullah, M., and Pradhan, G.K. "Efficient and Secure Information Sharing For Security Personnels: A Role and Cooperation Based Approach", International Journal on Computer Science and Engineering, Vol. 02, No. 03, 2010.

[18] NIST.gov — Computer Security Division — Computer Security Resource Center". Csrc.nist.gov. Retrieved 2010-08-09.

[19] MOPAS: Ministry of Public Administration and Security, http://www.mopas.go.kr/gpms/ns/mogaha/user/nolayout/main/english/userEngMainDisplay.action, Accessed Feb 2013.

[20] Public Information Sharing Center, news article (in Korean) http://www.dt.co.kr/contents.html?article_no=2006050102012060650002, May 6, 2006

[21] PISC Major Achievements and Results https://www.pisc.go.kr/fa/fa010/introduction/center_result.jsp

[22] Shafiq, B., J. Vaidya, V. Atluri and S. Chun, Information Sharing among Incident Management Systems using UICDS, Proceedings of the 11th International conference on Digital Government Research, 2010: pp 23-31

[23] Memorandom on Informing Consumers through Smart Disclosure http://www.whitehouse.gov/sites/default/files/omb/inforeg/for-agencies/informing-consumers-through-smart-disclosure.pdf

[24] Warner, J. and Chun, S. Privacy Protection for Government Mashups, *Information Polity: Volume 14, Editions 1 & 2*, 2009: pp 75-90.

[25] Citizens rail against government data sharing http://www.theregister.co.uk/2010/02/23/public_data_sharing_poll/

[26] Government scraps plans for citizen data sharing system http://www.computerweekly.com/news/1280093598/Government-scraps-plans-for-citizen-data-sharing-system

[27] Park, J. and Sandhu, R. The UCONABC usage control model. ACM Transactions on Information and Systems Security 7, 1, 2004: 128–174