Next Generation Electronic Record Management System based on Digital Forensics

Sekie Amanuel Majore[1], Hyunguk Yoo and Taeshik Shon[2]

Department of Computer Engineering, Ajou University
Woncheon-dong, Yeongton-gu, Suwon, Korea
{amanu97, cielo1025, tsshon}@ajou.ac.kr

Abstract

Due to technological advancement, it is very easy to generate electronic records within short period of time and with little effort. However, the challenge is to preserve electronic records for long period of time without losing their integrity and authenticity. This is critical problem because most of our day to day activities are dependent on the information we get from Electronic Record Management System (ERMS). The trustworthiness of electronic record is dependent on ERMS. Therefore, ERMS has vital role in keeping electronic record for long term without losing its trustworthiness. In this paper, we proposed novel approach for next generation ERMS that alleviates these challenges.

Keywords: *ERMS, Digital forensic, electronic records, integrity, authenticity, digital preservation*

1. Introduction

Technological advancement, especially in information technology changed the way records created, authenticated and preserved. It is estimated that more than 90 % of the records being created today are electronic [1]. Electronic records have different characteristics from that of physical records. Since electronic records require constant and continuous maintenance as they depend on hardware and software systems [2]. This makes it challenging task to preserve electronic records without losing their integrity and authenticity. The ability to rely on electronic records is an issue of increasing concern with the rise of formal e-commerce and e-government [3]. There is also trend of digitalization of historical records and making them available to public in national archives [4].

Trustworthiness of electronic record concerns professionals from different sectors. For instance, law enforcement bodies should prove any document which they use as evidence is reliable. Scholars also want to make sure any information they use for research is trustworthy. Similarly archivists have a responsibility to keep electronic records for long term without losing integrity, authenticity and being accessible. Electronic record is said to be accessible when user can read the electronic record using currently available software and hardware without problem. Similarly, digital forensic specialist work on digital device to preserve, collecte, validate, identify, analyze, interpret and document digital evidence derived from digital sources [7]. These methods also have been improving in terms of efficiency to cope with technological advancement that resulted sophisticated digital devices.

Currently, there are so many digital devices that contain important electronic records about organization and individuals which exist in different file format. It is not easy task to collect,

[1] First author
[2] Corresponding author

identify, validate and preserve these electronic records. Moreover, after electronic records are ingested into ERMS for long term preservation, it becomes necessary to migrate electronic records from one storage media to another to make them accessible despite of storage media degradation or obsolescence. Additionally, software which was used to create electronic record stops working on currently available operating systems or hardware. This problem also makes migration of electronic records from one file format to other file format necessary. Even though migration of electronic records solves problems related with technological advancement, it affects the integrity and authenticity of electronic record. When electronic record is migrated from one storage media to another can be altered unintentionally .But this can be avoided using well tested copying tools which are used by digital forensic specialists. Migrating electronic records from one file format to another file format changes bit stream of the electronic record .This process makes hash function based integrity checking mechanism of electronic records useless.

As result of technological advancement, migration of electronic record is unavoidable to make it accessible for long term. But any change introduced to bit stream of electronic record should not affect its acceptance as source of trustworthy information. Therefore, ERMS should make sure that electronic record does not lose its trustworthiness through time due to technological challenges.

In this paper we propose new digital forensic based ERMS which utilizes extensively digital forensic tools starting form ingest of electronic record to ERMS, transformation of electronic record for long term preservation. Additionally, when it is necessary to prove the trustworthiness of the electronic records, the proposed ERMS supports digital investigation in efficient approach.

The rest of the paper is organized as follows. Section 2 describes property of trustworthy records. Section 3 presents the proposed digital forensic based ERMS. Finally Section 4 concludes the paper.

2. Property of Trustworthy Records

A record to be considered as source of trustworthy information, it should be known at least when it was created and by whom it was created. Moreover, if the record was modified after its creation, this activity should also be documented properly. However, preserving electronic record for long term without losing its trustworthiness is challenging task.

The following are main properties of trustworthy electronic record.

- **Integrity** means that the record is complete and unaltered. This does not mean that records may not experience any changes, but it does mean that records must be protected against tampering or corruption and that it is clearly defined which changes or annotations might occur after the creation or capture of record [5].
- **Authenticity**: A record is authentic if it is what it purports to be and if it was created or sent by the person who claims to have sent it [5].
- **Proof of existence**: Specific techniques are required which can prove that an electronic record existed at a certain time in the past [3].

Basically these essential properties of electronic record are prepared using the bit stream of the electronic record, timestamp and hash function. A hash function takes an arbitrary string of binary data and produces a number, often called a digest, in a predefined range. Ideally, given a set of different inputs, the hash function will map them to different outputs [6]. After an electronic record is created, its digest (a number) is calculated by using bit stream of the electronic record. This number can be used for three purposes, first as means of integrity

verification mechanism. If an electronic record is modified after its digest is calculated, its bit streams will be changed as result its digest will be changed. Therefore, integrity of electronic record can be checked easily using its digest. Second authenticity of electronic record can be established using its digest and digital signature of its creator. Third existence of electronic record at a certain time in the past can be proved using its digest and timestamp form trusted timestamp authority.

The three techniques mentioned above which are used to prove trustworthiness of electronic record completely depend on bit stream of electronic. But technologically it is very difficult to keep bit stream of electronic unchanged in spite of technological advancement.

3. Digital Forensic Based ERMS

Next we will discuss three functional entities of the proposed ERM system as it is shown in the Figure 1. Basically the ERMS has three functional entities.

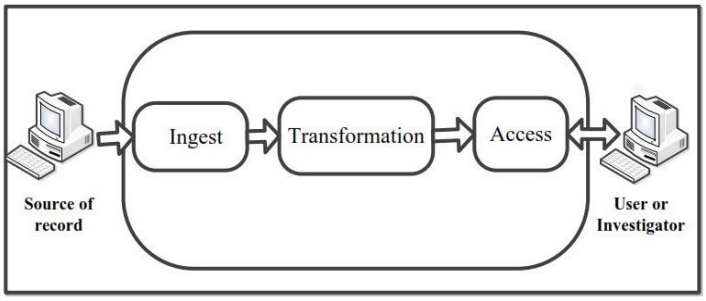

Figure 1. Digital Forensic Based ERMS

3.1. Ingest

In ingest functional entity electronic records are investigated by using available digital forensic tools before they are ingested for long term. Using digital forensic tools in ingest process is advantageous. For example, digital forensic tools can be used to identify files formats, encrypted file and date of creation. Especially this is helpful; when it is not possible to find necessary information about an electronic record during ingest process. Since digital forensic tools have powerful capability to work on different digital device which contain important electronic records. Therefore, using digital forensic tools as part of ERMS increases efficiency and capability the system.

3.2. Transformation

As we mentioned previously the two important challenges that make electronic record inaccessible are file format and media obsolescence .These challenges make migration electronic record from the original file format to another file and form media to another media mandatory.

The following activities are carried out in this functional entity; first the electronic record is copied form the original media to the other media which is supported by ERMS for long term. Digital forensic tool is used in copying process. Since digital forensic tools can copy digital data from media to another media with high accuracy.

Then the electronic record is migrated to file format that is chosen by ERMS for long term access.

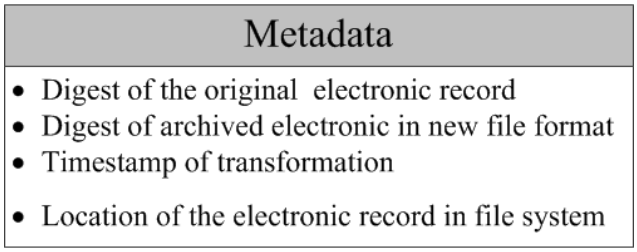

Figure 2. Metadata

During the electronic record migration to another file format and backup is taken all activities are done using the digital forensic tools to make sure that unnecessary or uncontrolled change is not introduced which affects the trustworthiness of the electronic records.

After the backup of electronic record in original format and new file format are taken. Then the next step is to prepare metadata about each electronic record in the ERMS .The metadata consists the following information about the electronic records; as it is shown in the Figure 2.

• Digest of the electronic record in original file format .The digest is calculated as soon as the electronic record is entered into the ERMS .Therefore; any changes introduced to the original electronic record after it is entered to the ERMS can be detected using the digest.

• Digest of the electronic record in new file format is used to protect the electronic record from any arbitrary changes since the electronic record is changed into new file format for long term long term preservation.

• Timestamp which is associated with important events related to the electronic records such as time of transformation.

• Complete information about the location of electronic record in the file system. This information is important. Because it helps to locate all electronic records easily when digital investigation is necessary.

Finally the following data are stored in separately with clearly defined access control to prevent unauthorized modification.

1. Backup of electronic record in original format
2. Backup of electronic record in new format
3. Electronic record which is directly accessible
4. Metadata of electronic record

3.3 Access

The access functional entity of ERMS makes available the electronic records for authorized user or digital investigation. Nowadays electronic records are vital component of e-governance and e-commerce. When any disputes arise concerning the trustworthiness of record found in the ERMS. This access point can be used to carry out the digital investigation in efficient way.

4. Conclusion

Nowadays, electronic records are being created by different organization and individual at large scale and due their digital nature, they can be modified easily unlike physical record as result they lose trustworthiness. These challenges make preservation of electronic records for long term overwhelming responsibility. In this paper we have proposed digital forensic based ERMS and how it utilizes digital forensic tools to preserve electronic records for long term without losing their trustworthiness.

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. 2012R1A1A1010667).

References

[1] Electronic Records and E-Discovery, "The Authority on Managing Record and Information", **(2012)** August 15, http://www.arma.org/erecords/index.cfm.
[2] A. J. Blazic, "Long Term Trusted Archive Services", Digital Society, First International Conference on the ICDS '07, **(2007)** January 2-6, pp. 29.
[3] J. A. Blazic, T. Klobuear and B. D. Jerman, "Long-term trusted preservation service using service interaction protocol and evidence records", Computer Standards and Interfaces, vol. 29, no. 3, **(2007)** March, pp. 398-412.
[4] Digitization and digital archives, "The National Archives", **(2012)** September 5, http://www.nationalarchives.gov.uk/about/websites-digitisation-digital-archives.htm.
[5] F. Boudrez, "Digital signatures and electronic records", Arch Sci , vol. 7, no. 2, **(2007)** June, pp. 179-193.
[6] V. Roussev, "Hashing and Data Fingerpringting in Digital Forensics", IEEE Security and Privacy, vol. 7, no. 2, **(2009)** March-April, pp. 49-55.
[7] G. Palmer, "A road map for digital forensics research. Report from the First Digital Forensics Research Workshop (DFRWS)", Technical Report DTR-T001-01,Air Force Research Laboratory, Rome Research Site **(2009)**.