Evaluation and Implementation of Digital Signatures to Improve Web Based Case Management System Information Security

A Case of Resident Magistrate Court in Dodoma-City, Dodoma Tanzania

Adolf Kamuzora
Department of Computer Science – College of Informatics and Virtual Education
University of Dodoma, UDOM
Dodoma, Tanzania

Hashim M. Twaakyondo
Department of Computer Science and Engineering – College of Information and Communication Technologies
University of Dar es Salaam, UDSM
Dar es Salaam, Tanzania
e-mail: hmtwaaky{at} yahoo.com

Abstract—**The paper-based infrastructure is one of the most fundamental and pervasive problems of administration of justice services delivery. With development of technology, Tanzania's administration of justice infrastructure has not advanced to keep pace with these changes to regulate their processes taking place in the modern age. Fortunately courts started to look toward integrated electronic Case Management Systems to cut down on quantity of paperwork and streamline day-to-day operations. However, these systems were old fashioned since less information security measures to guarantee stronger authentication, confidentiality, integrity and nonrepudiation were taken into consideration.**

Among the main challenges facing security measure implemented on Case Management System is the username-password authentication mechanism which is highly susceptible to social engineering attacks where a user may be tricked into revealing secret information used in authentication, hence leaving the system compromised.

This study has considered digital signatures technology would be the best solution to the aforementioned challenges. It provides mechanisms to detect unauthorised operations on electronic case information by enforcing encryption and signature application which result in stronger authentication, confidentiality, integrity, and nonrepudiation. Analysis of existing information security model was performed, resulting in implementation guidelines for an advanced information security model and subsequently a prototype which utilises Digital Signatures technology.

Keywords-Security, Integrity, Confidentiality, Nonrepudiation, Public Key Cryptography, Digital Signatures

I. INTRODUCTION

This template, Nature of the administration of justice or court system in Tanzania, which was inherited from British Colonial rule, contains common law principles which mainly facilitate paper based methods [1]. This administration of justice has not advanced to keep pace with these changes to regulate all activities that are taking place in our modern environment of electronic age. This creates an environment susceptible to mismanagement of case information in terms of tampering with such information and loss, since an enormous amount of information is dealt with day in and day out [2].

Efforts were made to mitigate this problem by introduction of Case Management System, [3] and Evidence Act No. 15 of 2007 (Written Laws (Miscellaneous Amendment) Act, Act No 15 of 2007) [4] that amends the Evidence Act No. 6 of 1967 [5] where electronic documents are now admissible in civil proceedings [6].

Laudon and Laudon [7] argue that this information system does not provide sufficient security mechanism for protection of case information. Such information security is in terms of Integrity, Confidentiality and Nonrepudiation, which are key aspects of information that give this information value and make it authentic [2]. Birme [8] argues that digital signatures technology of the public key cryptography system might provide a suitable technique to handle such challenges.

Whitman and Mattord [9] define Integrity as aspect of information assuring that is this information is not illegally altered as it traverses from sender to recipient, Confidentiality as characteristic of information that makes information private and Nonrepudiation as pinning a certain identity or user to signed information so that this user cannot deny later, this is false deniability.

In deriving such an information security model that addresses aforementioned challenges, the following issues have to be checked. These issues are i) What is the current process of information management in the court? ii) How does the implementation of Case Management System (CMS) facilitate case information security? iii) How would digital signatures improve case information security of court Case Management System to further dispensation of justice?

Previous studies by Laudon and Laudon [7] and Beard [3] have revealed that in most information systems, the security is enforced using username-password mechanism of authentication. Birme [8] argues that this model is weak as is highly susceptible to social engineering attacks which come in a form of causing someone to disclose secret authentication information without the valid user awareness. Also, once the user whether valid or invalid user, especially a systems administrator gains access into the system, all the information is viewable to that user and can do whatever he or she wants without detection.

This study aimed at reviewing the current mechanism of information security as described in other studies, working procedure of administration of justice and the CMS, discover further information security challenges faced, propose suitable alternatives to address those challenges and in turn a prototype for new requirements showing feasibility of the proposed solution.

II. METHODOLOGY

In finding solution to aforementioned challenges, authors were aided by the Security Engineering Life Cycle shown in Fig. 1. This formed the qualitative research design which helped to discover information security loopholes in both the flow of case information in the administration of justice and in the current CMS information security model applied, thus deriving new requirements for the proposed system. Then a prototype that illustrates how the challenges have been addressed followed.

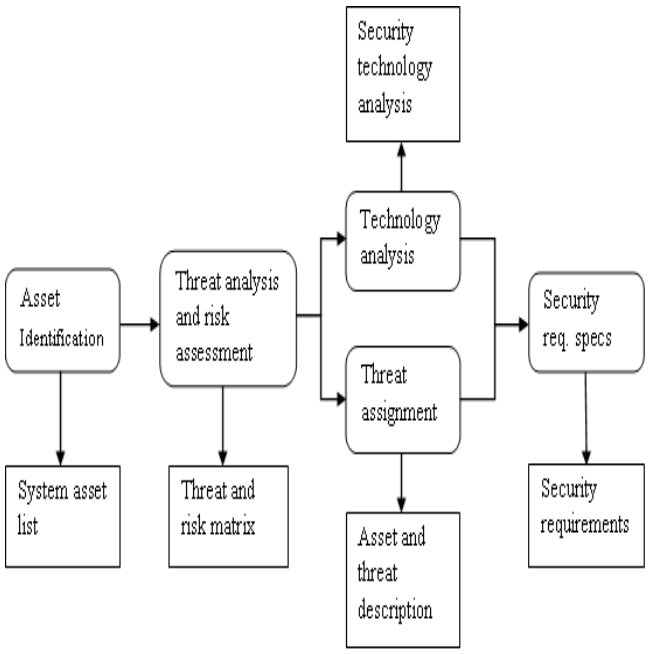

Figure 1. System Security Engineering Life Cycle. Source: [10].

In identification of assets stage the Resident Magistrate administration of justice assets and their required degree of protection are identified. Degree of required protection depends on the asset value so that for instance evidence information is more valuable than a set of public web pages. Also in an information system, data are the most valuable assets. They are usually a target of intentional attacks such as hacking. The most important aspects of data among others are authenticity, integrity, and confidentiality.

In threat analysis and risk assessment phase, security threats to administration of justice system were identified and the risks associated with each of these threats were estimated. Risks are associated with threats in a sense that risks to information systems are posed by threats in turn presenting possibility of attacks exploiting vulnerabilities of the system.

Threat assignment was a phase that encompassed mapping of identified threats which have adverse effects on characteristics of importance of data to assets of the court. These were related to assets so that, for each identified asset, there was a list of associated threats.

Technology analysis was stage that facilitated identification of available security technologies and their applicability against identified threats [10].

For the purpose of digital signatures implementation, 1024-bits RSA (Rivest-Shamir-Adleman) cryptography algorithm is used. This algorithm utilises very strong signing and encryption keys for digital signature application. RSA uses a pair of keys, a public key which is made known to many entities for verification of information authenticity and a private key for which integrity and most importantly non-repudiation would be strictly controlled since is only known and used by the owner of that key [9].

Another aspect of digital signature algorithm is the hash function. MD5 (Message Digest version 5) is among hashing algorithms that add a 128 bits seal or fingerprint to a document or message making sure it cannot been changed [11]. This algorithm is suitable in this situation since it ensures integrity of information.

For the case of bulk encryption RSA is not suitable due to its asymmetry, that is, since key pairs are used for encryption and decryption respectively. Whatever public key encrypts private decrypts and vice-versa [9]. Kapis [12] argues that Advanced Encryption Standard (AES) or Rijndael-128 is a symmetric encryption method that is efficient since handles bulk information well and is current state of the art technique used. This technique makes case information unintelligible thus confidential and can only be read by parties who are in possession of or have shared the respective key.

With respect to the technologies described above, a protocol suitable for use in the proposed information security model is the Pretty Good Privacy (PGP) protocol. PGP utilises RSA public key cryptography combined with symmetric key cryptography facilitating public key digital signatures and bulk data encryption. Another protocol that is used was the Secure Hyper Text Transfer Protocol (S-HTTP) that enables RSA

encryption of information in transmission thus protecting it from third parties eavesdropping in the middle of data transmission or as it shifts from one concerned party to the next.

III. RESULTS

Fig. 2 is a context diagram portraying Resident Magistrate (RM) administration of justice case information flow and personnel who participate in case management. Case information since inception of a case to ruling is moved around the external agents portrayed in the context diagram.

Advocates are people who represent people who sue each other in a case. This is a point where cases start by an advocate submitting a complaint thus suing another person. The complaint is reviewed by a registrar of the administration of justice, and then registry officer opens a case file in the Case Management System and assigns this case to a judge. This file contains categories of information such as evidence, copies of summons, receipts of case file access, complaint statement, Written Statement of Defence (WSD), decree and proceedings written by the judge. Case information in this case file shifts a lot as illustrated in Fig. 2 among parties shown.

Such case files access and shifting exposes this information to different risks that potentially compromise integrity, authenticity and confidentiality as the most important characteristics of information that give it value. Therefore appropriate controls that address the risks were put in place.

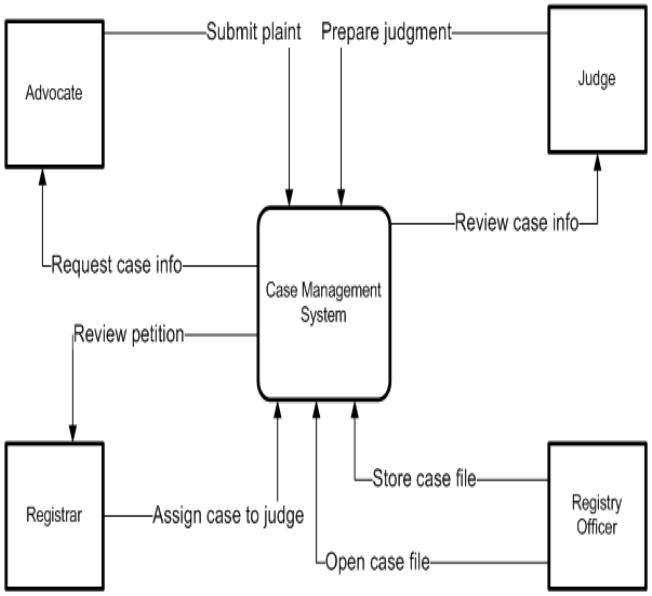

Figure 2. Context Diagram for Case Management System.

A. Asset Identification

Case information is the most important asset in the Resident Magistrate administration of justice. These assets have already been mentioned in the previous section while describing flow of case information in case management.

Evidence, decree and plaint are the most valuable assets and require the highest degree of protection in all aspects of integrity, confidentiality and authenticity. Court order, judgment, plaint and WSD require medium level of secrecy with summons having the lowest level of protection in terms of confidentiality characteristic.

B. Threat Analysis and Risk Assessment

As described in the methodology section, threats to the court Case Management System, especially to case information are illustrated in Table I with their likelihood of risk.

As par the Table I there is a high likelihood of a party to alter contents of case information and to even remove them. There is a medium chance case information which is to be kept confidential could be illegally exposed to other parties among court staff and opposing counsels.

C. Threat Assignment

In this phase, RM electronic assets with associated threats to them were identified. Table II illustrates electronic assets on the first column mapped to threats directly affecting them with an order of applicability in the second column. Numbers in the second column mark a threat illustrated in Table I that apply to particular electronic assets.

For instance, a plaint is directly associated with threat 1 and 2 as illustrated in the previous Table I in a sense that its contents could intentionally be modified and that its contents could be partially or entirely removed rendering the plaint useless.

TABLE I. THREATS/RISKS TO THE RM COURT CASE MANAGEMENT SYSTEM

Table Head	Threat/Risk	Likelihood of occurrence (High, Medium, Low)
	1. A user (administrator or normal user) could intentionally or by mistake	Medium to High
	2. The contents of a case document could either be overwritten or removed	High
	3. Information pertaining to a certain case could be leaked to staffs who are not involved	Low to Medium
	4. Information could be leaked either to the public or opposing counsels.	Low to Medium

TABLE II. LIST OF IDENTIFIED RM COURT ASSETS ASSOCIATED WITH IDENTIFIED THREATS/RISKS

Table Head	Asset	Associated Threat/Risk (1, 2, 3, 4)
	1. Evidence	1, 2, 3, 4
	2. Plaint	1, 2
	3. WSD	1, 2
	4. Summons	2
	5. Judgment	1
	6. Court order	1, 2
	7. Decree	1, 2

D. *Technology Analysis*

For Signature, hashing and encryption algorithms explained in the previous section fall into PGP protocols. Similar to the previous section, applicability of these protocols is summarised in Table III showing protocol, algorithm and what threat/risk that was addressed by the respective algorithm. Values in the third column stand for threats identified in Table I

Par Table III 1024-RSA and 128-MD5 signature and hashing algorithms address threats/risk 1 and 2 that is dealing with any unauthorised alterations to contents of case information with an application of a digital signature. AES-128 encrypts case information to make it confidential when it is stored in a CMS and 1024-RSA of S-HTTP is used to encrypt case information as it is moved from one party to another so that it cannot be leaked.

With the above analyses, discovered requirements for the proposed information security model which address the challenges should cater for advanced authentication up on accessing the CMS. Users will have the ability to digitally sign case information for purposes of non-repudiation and integrity thus making information authentic and cater for bulk encryption so as to make case information confidential among concerned parties.

TABLE III. PROTOCOL AND RESPECTIVE ALGORITHMS ADDRESSING IDENTIFIED THREATS/RISKS

Table Head	Protocol	Algorithm	Addressed
	PGP	1024-RSA	1, 2
		AES-128	3, 4
		128-MD5	1, 2
	S-HTTP	1024-RSA	3, 4

E. *User Authentication*

From the original design, a user is authenticated using username and password. In addition to having correct authentication information, in the new information system security model, a user wishing to gain access to the system is also supposed to have a valid digital certificate in possession. Therefore, the new user authentication model applies multi-tier authentication in which in the first level user and server need authenticate themselves by presenting valid digital certificates to each other in a mutual certificate authentication handshake. The user will be confident that he or she is accessing the correct CMS website and the server will be assured of the identity of the user wishing to be authenticated into the system.

In the authentication as illustrated in Fig. 3, client first requests a resource from a protected area, then the server will present itself with a digital certificate to the client. The client will then check in a public trust store which is usually a Trusted Third Party (TTP) to verify that the server identity is valid then the server will request the client to present itself with a digital certificate that has a valid signing key. The server checks with a trust store to verify that the client is valid and thus recognised by this TTP. Up on successful handshake, client will now be presented with an interface that will enable supply of username and password to complete the authentication process.

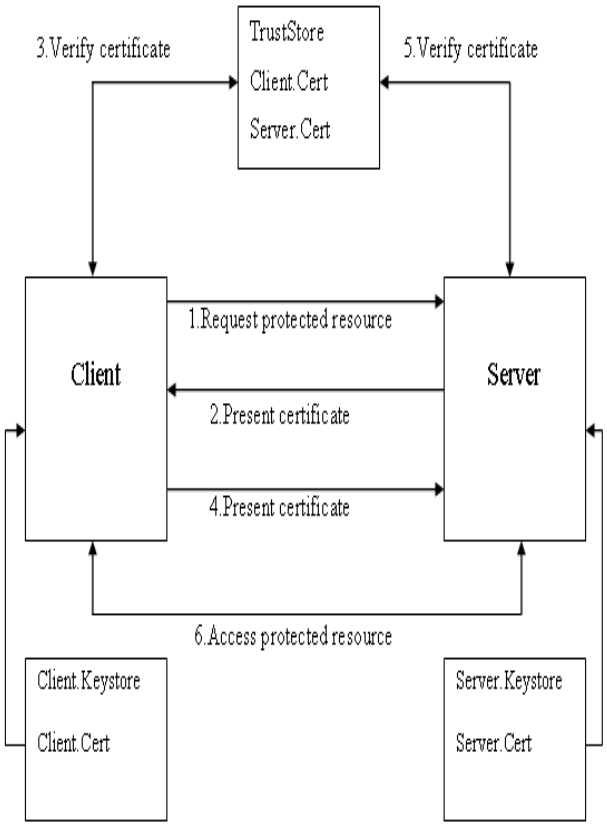

Figure 3. Client-Server mutual authentication handshake.

Fig. 4 and Fig. 5 demonstrate client-server mutual certificate authentication process. In Fig. 4 the server first presents its digital certificate to the client. In Fig. 5 the client is requested by the server to present itself with a certificate. This client certificate is actually personal information exchange encoded containing certificate and private key of the client.

F. Nonrepudiation Mechanism

A mechanism to prevent false-deniability, this means that the user can still tamper with information, but he/she can never falsely deny what has been done, called non-repudiation. This is illustrated in Fig. 7. A private key is used for digitally signing case information. To this point since the user has passed the advanced multifactor authentication levels, it is true that this user has a valid signing key. In the current security model, digital signature application was not incorporated. In the proposed system the authenticated user is compelled to digitally sign information that had been supplied into the CMS. Such a mechanism ensures that there is an audit trail. This will let other users of the system know which information was verified authenticity by whom and therefore it can be attributed to that person.

Such a mechanism would also ensure other users of the case information that such information has been verified by a valid system user and thus such case information to be valid and authentic. If there was a violation a user who previously signed such information would be held accountable since the information has been digitally signed.

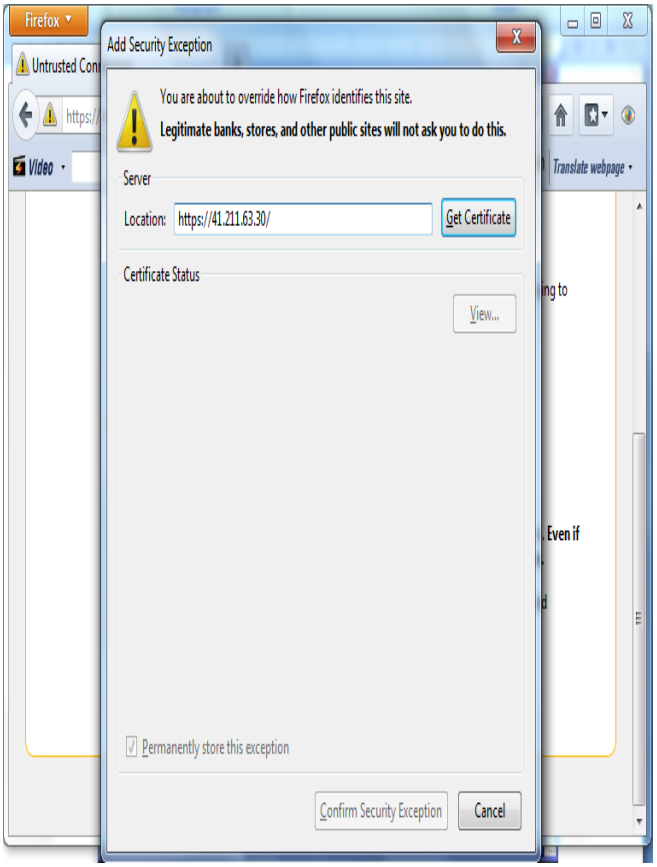

Figure 4. Server identifying itself with a certificate.

G. Access Control

Access control is usually associated with restrictions in information flow which assures confidentiality of case information. This means in the Case Management System it is required that information is only accessible to concerned parties. Unfortunately in the current system, the system administrator who might not be involved in a particular case still has access to confidential information since he is responsible for continual operating the CMS and environment surrounding the system.

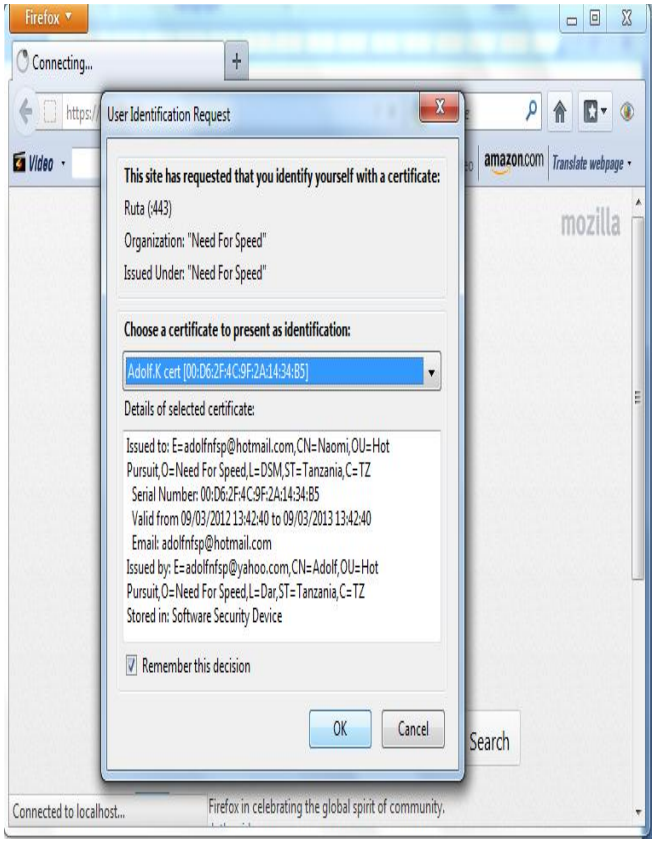

Figure 5. Server requesting client to identify itself with a certificate.

Public/private key pair is concerned with information authenticity and integrity. For the case of confidentiality, a symmetric (or shared secret) key is appropriate since it is able to perform efficient information encryption or that it can perform encryption of bulky data.

In the proposed security model, a user wishing to share confidential information with fellow users on a particular case even without the administrator knowing what is going on, first would encrypt the information using a secret symmetric key making case information unintelligible. Then this user will encrypt this symmetric key using his or her fellows' public keys since the public key is distributed freely. The user would thus create something referred to as a digital envelope as illustrated in Fig. 6.

To recover the symmetric from that digital envelope, the recipient would have to use his or her private key which is only known to that user to decrypt the key information.

Confidentiality would be maintained since this user is the only one who can reveal case information addressed to him or her since what was initially encrypted with a public key of that user can only by decrypted by private key of that user and the private key is only in possession by that user.

Fig. 8 is an interface that illustrates an implementation of the security model enforcing access control of case information and thus making it confidential. Symmetric key is encrypted with a public key of a recipient and then it is later decrypted using private key by that recipient.

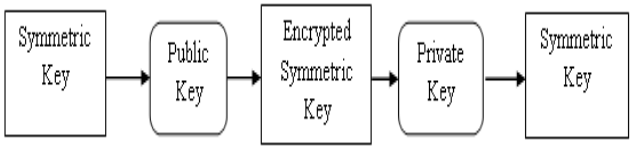

Figure 6. Digital enveloping of a shared secret (symmetric) key.

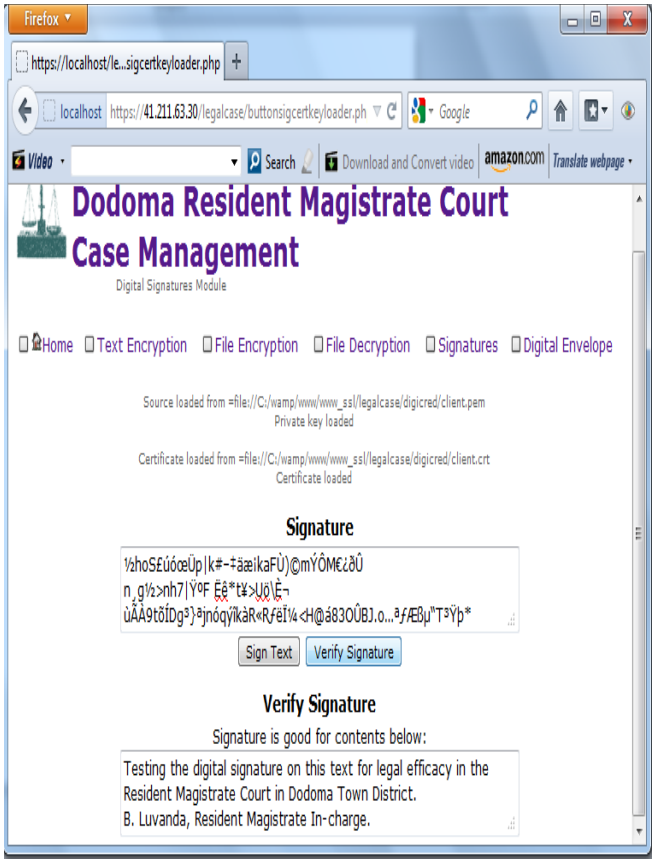

Figure 7. Digital signature application and verification.

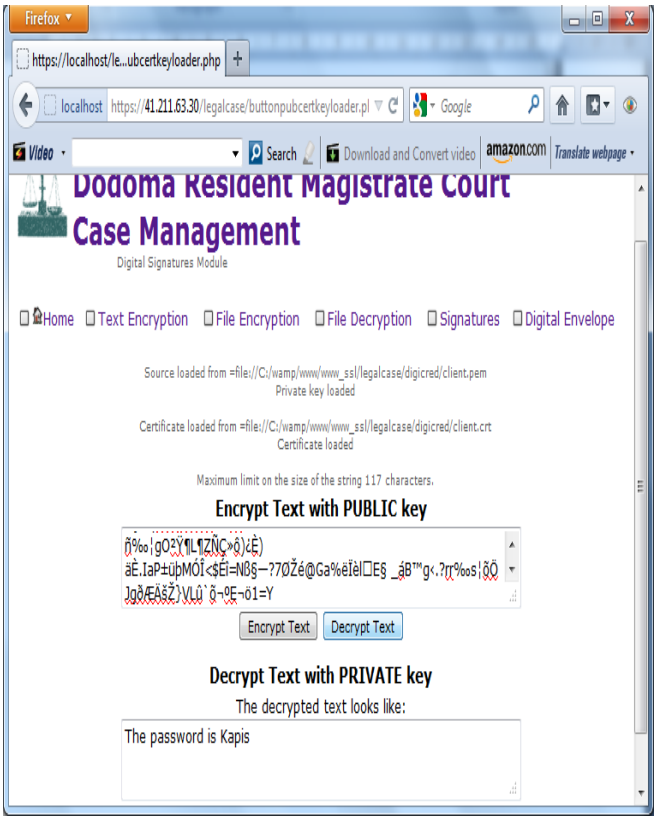

Figure 8. Encrypting a symmetric key with public key of intended recipient.

IV. DISCUSSION

User authentication, integrity, non-repudiation and confidentiality are some of the critical challenges that a RM administration of justice CMS faces. Some of the suggested approaches that [7] shown have worked well, still a better way was advised.

Current CMS compared to the proposed system by this research study has shown that security of information in terms of authenticity, integrity, non-repudiation and confidentiality attributes has improved. Current systems offered username-password means of authentication, information was communicated through unsecured channels and means of access control for confidentiality was through access levels. The access levels are administrator, normal user, external user and closed user. Also there was no means of encrypting information and attributing who might have accessed information last since no signature capabilities.

The CMS information security method proposed in this study addresses well the challenges faced. In the case of authentication, in addition to a user whether being registrar, registry officer, advocate, judge or administrator accessing the system using username and password, is also supposed to be in possession of a valid signing key that will be used for signing case information. With a digital certificate that comes with the signing key will make the server be sure of the identity of that user since the certificate used is also known to TTP. Since this user is supposed to digitally sign case information using private key, the information signed would automatically be attributed to that person, thus enforcing non-repudiation. Public keys of users are also used to encrypt secret information that could only be decrypted by a recipient possessing a corresponding private key. Therefore confidentiality is maintained since only the person who has the private key only possessed by that user may decrypt that information.

To better illustrate how the information security mechanisms implemented work, users evaluated and tested the system with possible attacks against the proposed system. This would show that CMS information security challenges that presented potential compromise to the system have been addressed. Evaluation was based on both Social Engineering and Man in the Middle Attack techniques. Social Engineering technique required the user to have the ability to influence and persuade people to reveal secret authentication information while remaining composed under pressure. Man in the Middle Attack technique required extensive TCP/IP, networking knowledge and techniques to evade detection.

Social engineering technique was used to learn passwords of users to use for logging in the system. The user was required also to authenticate with a digital certificate that has a valid signing key. Thus authentication failed since the illegal user was not in possession of such digital certificate.

Also Man in the Middle technique was to be used on evaluation; unfortunately users lacked the necessary skills for this technique. However in theory to perform a Man in the Middle Attack, the user intercepts information on transit and reads it. The system works in a Secure Sockets Layer (SSL) using Hyper Text Transfer Protocol (S-HTTP) protocol where the channel is secure using 1024-bits RSA algorithm. Hence the information on transit is encrypted. Thus the mechanism to hide information from unauthorised users was also effective and proved to have advanced access control mechanisms.

Based on results obtained and discussed, the proposed system has shown to address aforementioned challenges and thus providing a more stable model for secure access and utilisation of case information in the CMS. This system offers services that cater for advanced authenticity, integrity preservation, making case information confidential and audit trails.

Despite aforementioned achievements of this study, there are still some other challenges that require attention to better the proposed security model. First there is an issue of TTP and how key repositories would be managed. Secondly, it is suggested that case information not be deleted so that the issue of audit trails would work effectively. Information is digitally signed and versions of case information are retained, which enable to trace from the first version of case information to the last.

V. CONCLUSION

This research paper has evaluated the information security scheme that was applied on CMS. In the evaluation process the aim was to review current scheme of case information management in court Case Management Systems so as to improve existing mechanism of securing case information to further dispensation of justice. Results of this research have shown that digital signatures would be a suitable choice for addressing the challenges that motivated this research. The challenges were lack of mechanisms to address confidentiality, integrity and non-repudiation aspects of information security in CMS.

The basic promise of digital signatures is that through implementing this electronic innovation, there will be enhanced efficiencies in case information protection, signing and management process. As stated at the outset of this paper, case information management process is subject to inefficiencies such as spending much time in verifying information dealt with. By mitigating these inefficiencies, the hope and plan is to aid administration of justice staff in focusing on the value of their services and efficient service delivery.

VI. FUTURE WORK

Despite the achievements shown, there are still other challenges that require attention to further the proposed information security model. First there is an issue of the TTP and how the key repositories would be managed. Secondly, it is suggested that case information should not be deleted so that the issue of audit trails could work effectively. Information is digitally signed and versions of case information are retained, which enables to trace from the first digitally signed version of case information to the last. Thirdly, files used for case information were text files since most of case information assets comprise statements. The model could be improved to incorporate files of other formats.

ACKNOWLEDGMENT

The authors would like to thank the staff of Resident Magistrate Court of Dodoma City. They made available all documents required by the researchers at any time when they were in need of them. They were also available for interview when ever appointment was set. Without their support, this paper could not have reached this stage.

REFERENCES

[1] A. Mambi, "An overview of the legal implications of information and communication technologies in Tanzania: a comparative perspective," Tanzania Lawyer Journal, 2-JTLS, pp.88-91, 2008.

[2] J. Ubena, "ICT as a solution to delay of cases in the administration of justice in Tanzania," Tanzania Lawyer Journal, 2-JTLS, pp.116-118, 2008.

[3] J. Beard, "An open source system for electronic court filing," [Online] Available from: http://www.linuxjournal.com/article/7441 [Accessed 30th June, 2011], 2004.

[4] Evidence Act No. 15 2007, Written Laws (Miscellaneous Amendment) of Evidence Act 1967, Tanzania, 2007.

[5] Evidence Act No. 6 1967, Evidence Act, Tanzania, 1967.

[6] J. Ubena, "Why Tanzania needs electronic communication legislation: law keeping up with technology," Law Reformer Journal, No.1 Vol.2, pp.17-26, 2009.

[7] K. Laudon and J. Laudon, Management Information Systems: Managing the Digital Firm, Dorling Kindersley, India, 2007.

[8] J. Birme, Document Management System Security, M. Sc. Computer Science thesis, UMEA University, Sweden, 2005.

[9] M. E. Whitman and H. J. Mattord, Principles of Information Security, 4th ed., Congage Learning, USA, 2011.

[10] I. Sommerville, Software Engineering, 8th ed., Addison-Wesley, 2006.

[11] K. Kapis, and S. P. Korojelo, "Online surveys system with enhanced authentication intelligence: a case of online course evaluation system," International Journal on New Computer Architectures and Their Applications (IJNCAA), 2(1), pp.81-90, 2012.

[12] K. Kapis, J. C. A. van der Lubbe, and K. Cartrysse, "Cryptographic approach to patient records privacy protection in emergency situations," In Twenty Fifth Symposium on Information Theory in the Benelux, pp. 177-184, 2005.