Grenze International Journal of Computer Theory and Engineering , Oct 2017

Catastrophic Of Data in Health Care Organizations. A Solution - "By A More Secure Mechanism with Dual Authentication Based Scheme"

Uthamakumar[1], Meenakshi[2] and Satish.E.G.[3]
[1]CMR University/CSE dept, Bangalore, India.
Email: uthamakumar.15phd@cmr.edu.in
[2-3]Nitti Meenakshi Institute of Technology/CSE, Bangalore, India.
Email :{ Meenakshi, Satish.e.g} @ nmit.ac.in

***Abstract*—"Cloud computing provides ubiquitous and on-demand computing of provisioning and de-provisioning of re-sources to the consumers based on pay-per usage in all the sectors." Most health care organizations deals with large sets of data, highly imposes to data vulnerabilities leads to insecurity of data, thus confidentiality of data can be achieved by the use of encryption-and decryption mechanisms with the use of asymmetric key cryptography, which possess both authentication and confidentiality. With the use shared secret key between of key pairs of asymmetric key cryptography such as private/public key pairs are not in identical and it is known to the augmented users only. Public-key can be known to any-one such as known as public-key cryptography; and with private key the encrypted data is decrypted by the actual owner who owns it.Even with private-key digitally signed as the user is authenticated and it shows the proof-of-identity for the system. Key-pairs are distributed by KDC to the intended users only. With AS (authentication-server), present in key-domain authority (KDA) of KDC acts as dual-authentication/authorization for the endorsed key as along with digital signature of the message and digital certificate is issued by KDA thus the Digital ID will be generated in hashed format with SSO.Thus, by means of dual-authentication based schemes it proves to be more secured for the given messages. Thus, Managed PKI which manages the keys , grants/access, revokes certificates provides a secure authentication and reliable communication in a specific cloud based platform to be in a secured way, by means of the use of dual-authentication based schemes such as in with {((key, message, Digital signature), Digital certificate)}and {message, (key), Digital$_{(Id)}^{h}$}; to gain a secure cloud environment mainly in health care organizations to provide a better cloud services to the cloud users by in a protected cloud environment.**

***Index Terms*— KDC, KDA, AS, Digital Signature, Digital Certificates, Digital ID's, managed PKI, Kerberos protocol, TGT, TGS, RFC (Request for Comment) 4210.**

I. INTRODUCTION

"Cloud computing provides provisioning and de-provisioning of resources to the cloud users with the intact of CSP (Cloud Service Provider). End users in the cloud handles huge data of diabetic care of patients in

Grenze ID: 01.GIJCTE.3.3.501

health care organizations poses to many threats such as it leads to many cloud security issues[1] such has confidentiality, integrity of data in terms of use of EHR, EMR, PHI."Privacy is a main concern when it comes to electronic health records. Using EHR[2] software can put your organization in risk if not followed certain privacy protocols[3],[4] to a certain level of degree such as Microsoft Health vault, health care services. Even paper records can be violated of patient's data to an undimensional level.

Data theft occurs when an unauthorized people have access to private data. Even a dishonest person can use the patient data and commit it to fraud. Even, EHR software alone is not a main concern to blame for data misuse in the health care organizations in case of paper records of diabetic care of patients scenario also leads to an unpleasant level.Loss of data is a main privacy by the use of EHRs. A system crash can wipe out all vital data stored in for several years, creating a tension for all the staffs ability who are maintaining the patients data for several years and so there is a need of a robust backup plan such as to maintain cloud offsite backups for their data through a CSP. Even local servers can cause of catastrophic data crash to an unreasonable level, so there is a need of cloud back up storage sites. "Cloud computing is a developing paradigm, its definition, attributes, characteristics will evolve over a time. Vaquero et al studied more than 20 definitions and tried to extract a consensus definition as well as a minimum definition containing the essential characteristics. Based on the study, they defined cloud computing as follows:"

From services point of view, cloud computing has 3 archetype-pal models or services: software, platform, and infrastructure [5].

1 .Software as a service (SaaS): The applications (e.g., EHRs) hosted by CSP are in use to customers through a network, such as typically by the Internet [6].

2. Platform as a service (PaaS): The development tools (e.g., operation systems) are hosted in the cloud can be accessed through browsers. PaaS developers can build their own Web applications without the use of any tools on their computers, can build and deploy their own applications on it and doesn't requires any specialized skills.

3. Infrastructure as a service (IaaS): The cloud user outsources the equipment to support operations such as storage, hardware, servers, networking components and he or she is responsible for housing, running, and maintaining it and pays it based on a pay- per-usage model.

"With new innovations, cloud computing should be rigorously adapted to various levels. Based on some research papers they systematically studied the effect of cloud computing on health care IT in terms of its opportunities and challenges based on the viewpoint of management, technology, security, and legality."

This paper mainly deals with confidentiality of data mainly in health care organizations with respect to diabetic care of patient's data stored in the cloud. By use of asymmetric key cryptography, role of shared secret key, with key pairs, Digital signatures, Digital Certificates and Digital ID's generated for the given messages and by means of efficient use of managed public-key Infrastructure with its roles and it's capabilities. Such as, it manages the keys, accesses it, performs roles on digital Id's creation/revokes/grants and manages them efficiently known as Key-process-creation management done by KDC and KDA, AD (active-directory),TGT(ticket granting ticket),TGS (ticket granting server).It has the following sections such as Section 1:Related Work or Literature Studies. Section 2: Motivation. Section 3: Problem Domain. Section 4: Problem Definition. Section 5: Statement. Section6: Innovative Content. Section 7: Problem Formulation or Representation or Design. Section 8: Solution Methodologies or Problem Solving. Section 9: Results and Sensitivity Analysis. Section 10: Conclusion.

A.Related Work or Literature Studies.

"Confidentialityof data refers to only authorized parties having the ability to access the protected data. The threat of data compromise is high in a cloud due to the increased number of parties, devices and applications involved, that leads to an increase in the number of points of access. Delegating of data control in the cloud, inversely leads to an increase in the risk of data compromise as the data is accessible to a number of augmented parties. Many concerns arise regarding the issues such as of multitenancy, data remanence, application security and privacy [8]. These can be controlled by Trusted Third Party Services and by managed PKI within the cloud by providing Trusted level services[9] to the users to preserve the confidentiality, integrity , authenticity of data and communications [10] (Fig. 1) not only by technical, but also by legal, financial, and structural means [11] ; [12]."“Eight years ago, it was all about securing applications within the enterprise through identity management. Today we talk about securing applications in the cloud with identities originating within the enterprise [13]."“Cryptographic Separation is in which processes, computations and data are concealed in such a way that they appear intangible to outsiders [14]."

“A key distribution Centre (KDC) in cryptography is a system that is responsible for providing keys to the users in a network that shares sensitive or private data. Each time a connection is established between two computers in a network, they both request the KDC to generate a unique password which can be used by the end system users only for verification.”Cryptography is the main art of realm of security with encoded messages to make them non-readable [15] to the other non-intended users. With asymmetric key cryptography of private/public key pairs are created by KDC and it is distributed to the users, thus it is shared b/w the sender and receiver only with the intact of the shared secret key. Anyone can use the public key and can send any no.of messages to the receiver .Messages that it is in encrypted form is decrypted by the intended receiver only by the use of private key owned by that actual sender. Key-domain authority present in KDC has AS (authentication server), it has TGS and TGT done by means of through a security principal RFC (Request for comment) 4210. Through AS, user is authenticated and authorized such as dual-authentication , the TGT is issued to the intended user by means of TGS to the intended user can only access or store the data in to the cloud. By the efficient use of managed PKI mechanisms and it’s roles as part of with health care organizations in terms of using of patients data. In AD (active directory) all the authenticated user’s list of information is stored along with their keys generated, key-revocation lists, key-deletion etc., and all of the current users are updated in to AD.

Asymmetric key cryptography is also termed as public key cryptography. Even, if the public key is known the contents present in the original message can be known to the fraudulent users based on the network leads to data vulnerabilities. Public key can be known to anyone and it will be in encrypted form, can only be decrypted by the private key of the user who actually owns it, thus it shows the proof of Identity of the system. Even if the private key is signed in as for message authenticity, digital signature is generated for the given message and as along with digital-certificate is generatedsuch as digital Id is created for the given message and it will be particularly stored in hashed format. The original message in encrypted form is compared with digital signature of the intended message and it is also compared along with the digital id or digital certificate created for the given message; can only be decrypted by through private key known b/w the intended users such as by the acts and roles of KDC, KDA. Even if the secret key is known he or she can decrypt the message leads to data misuse. Thus, by means of dual-authentication based schemes can be more secured and thus it proves to be an even more secured process with general in context of information to be stored in or accessed from the cloud.“Key distribution and authentication Protocols are divided into two categories to verify the authenticity of a message. First category uses nonce and challenge/ response handshake protocol to verify the authenticity of messages. Second category uses timestamps to all the machines in distributed system are in clock-synchronized to secure the machines with by MIM attacks on it; example of such is known as Kerberos Authentication Protocol [16].”Even digital signatures can be forged out by means of adaptive chosen message attacks on it; Thus digital certificates or Digital IDs generated and stored in standard hashed format and by the efficient management of PKI can be an even more proved to be a more secured cloud environment.In any of these cases, an unauthorized user may be able to gain access or services to data that he or she is not authorized to access the data. So, thwart of these the digital signatures , digital certificates and digital ID’s mainly in hashed standards can be an considerable proven security to access the patient’s data in terms of use of (EMR, EHR, PHI (personal health Information)) software in a secured way. And also mostly, even by use of multi-authentication based schemes we can achieve an even better higher secure cloud data mainly in health care organizations in a better and efficient way to be known as a secured cloud care.

B. Motivation

My proposed scheme of dual-authentication based schemes based on digital signatures, digital certificates and digital ID’s can be a more secured cloud environment with such as by cloud offerings , cloud services to the consumers mainly in health care organizations in access of data retrieved or collected from diabetic care of patients data in a huge manner from the cloud. Thus, the data is secured in the respective cloud environment, where the authenticated user only can access his data. By through AS, where the private key is signed in, and by dual-check authentication done by through digital signatures , digital certificates and digital ID’s generated can to be in a secured way. Even in case of DDOS attacks also, the intruder can’t decrypt the data accessing by the client, due to the dual-authentication based schemes of digital ID and digital signatures generated and stored in hashed sequences for the respective given messages.User’s signed digitally as with digital signatures and digital ID can be a highly secured cloud environment in clouds utilized by the consumers and to compute those Digital ID’s along with digital signatures generated for the given messages

it takes a high computational time. Thus the data is more secured in a cloud environment to gain the confidentiality of data in various source clouds.

C. Problem Domain

In asymmetric key cryptography key pair's such as Priv $_{K}$ey, pubkey are created and managed by shared secret key. If the secret key is known, we can decrypt the original message. Thus, by private key is digitally signed in and it is checked by the AS(authentication server)for means of dual-authentication to be a better secure process or mechanism in confidentiality of data, and it is distributed to the authenticated users only by KDC,KDA for dual-security principle. Such as with digital signatures for the given messages signed in and with digital ID's generated in and stored in hashed formats can be proved to be a highly more secured cloud environment in case of data vulnerabilities happening in the cloud.

D. Problem Definition

Even if the signed priv$_{K}$ey is known by the intruders through MIM,DDOS attacks they can decrypt the message which is mainly shared b/w the intended users can also, who are they authenticated and authorised.By chosen adaptive message attacks on the Digital signatures can guess the private key to unlock the data present in the given message. By means dual-authentication b/w the DS(digital signature) and Digital Id can be achieved a better data protection. Even if they know, it seeks for the digital ID (i.e. in password) generated for the given message and stored in hashed sequences. To compute those messages it takes a longer time for the malicious intruders or eavesdroppers to guess the key for to decrypt the data. Thus, by use of dual-authentication based schemes, it can be achieved and be secured to a greater level of extent, thus confidentiality of data is maintained to a maximum level.

E. Statement

Thus Managed PKI which manages the keys , grants and gives accesses, revokes certificates to provide a secure authentication and reliable communication in a particular cloud based platform in a secured way thus by the use of dual-authentication based schemes. Given such as with {(key, message, Digital signature), Digital certificate)} and (message, (key), Digital $_{(}$Id) ^{h}) to provide a better secured cloud environment mainly in health care organizations.

F.Innovative Content

Mainly digital ID's in hashed formats can be a newer novelty technique as with digital signatures and digital certificates by dual-authentication based schemes can be a even better solution for data vulnerabilities happening in the cloud, to be reduced to some level of extent with by use of asymmetric key cryptography encryption and decryption standards. In more general specific even multi-authentication based schemes can be evenly better choice in case of data anomalies happening and governing in the cloud.

G.Problem Formulation or Representation or Design

Alice

(Sender/owner)

Bob

(Receiver)

Alice got key pair's by KDC such as A = {X_A, Y_A} .Private Key is {X_A}, Public Key is {Y_A} and shared secret key is K.	Bob can decrypt the message by use of public key of Alice. Then B = { Y_A}.
By AS → Alice is authenticated, private key is signed and Digital ID is created such as A = {X_A, ($X_{AS,}$ X_{ADC})→X_{AD} }. $X_{AS}$is digitally signed; $X_{ADC}$is digital certificate for the signed private key, X_{AD} Digital ID in hashed format.	By use of secret key to decrypt the message, Bob still needs private key of Alice to decrypt it. Now B = { Y_A, X_A}. Alice private key is signed and it needs digital ID.

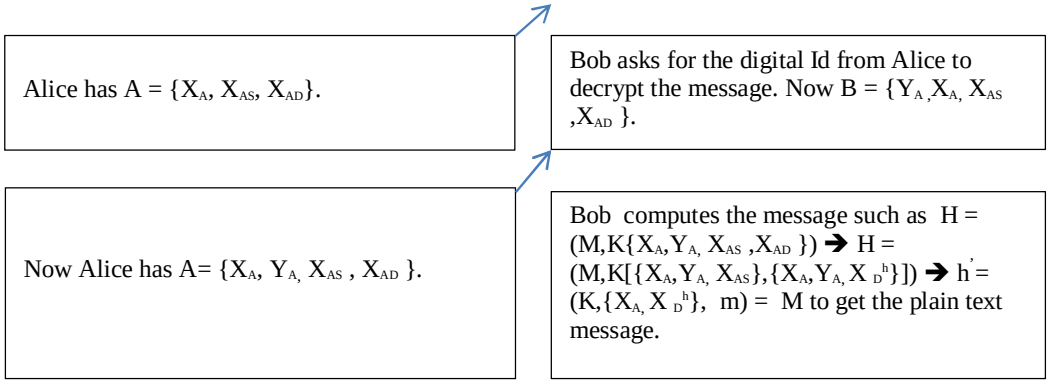

Figure 1. key - process - and – Management

H. Solution Methodologies or Problem Solving

For the given message M key pairs are created with the use of asymmetric key cryptography and it is distributed to the intended users by KDC, and it is efficiently managed by Public Key Infrastructure (PKI) such as it maintains the key management, key distribution mechanisms and by KDA present in KDC is used to provide authentication and reliable communication on a specific cloud platform with dual-authentication check standards or mechanisms. Such as with

$$(X_A , Y_A)$$

Where Priv $_K$ey is (X_A), Pub $_K$ey is (Y_A). Where Priv$_K$ey (X_A) is signed in proves to be the proof-of identity for the system as a single-authentication. Key-domain authority present in KDC has AS, enables that the user is again authenticated and authorized to send or receive the messages with a SSO(single-sign on) as a dual-check authentication for to be a more secure and protective mechanism when dealing with data in cloud and not to happen any data anomalies. When a private key is endorsed in as with AS digital certificate is issued by KDA, as well as long with digital ID is created and stored in hashed format. Digital signature generated for the given message by KDA of being by AS a dual-check authentication, is created and it is provided to the sender by KDC and by efficient manage of PKI.Thus, sender has both key pair's, Digital signatures, Digital certificates and digital ID's generated for the given messages. If the receiver wants to decrypt the message sent by the sender he must know the private key asendorsed in, as with digital signature and digital ID generated for the given message is known by that actual sender only. Thus sender shares it to the receiver through the role of shared secret key. Even if public key is known he can easily deduct the private key and he or she can easily judge the digital signature for the given message by chosen adaptive message attacks thus to know the actual contents present in the original message and thus it leads to inaccuracy of data. By, through digital ID message authenticity and authorization is achieved, thus confidentiality of data is maintained. And it is even more secured with dual-check authentication based schemes, such as within (message ,(key), Digital signature, Digital certificate) and (message, (key), digital Id^h).Even if the secret key is guessed and digital certificate is known by MIM attacks also he or she can't decrypt the message and thus it still asks the digital ID created for the given message to unlock the data present in the given message to finally decrypt it completely and thus it is known by that actual sender only is shared to the receiver with the role of shared secret key between the augmented parties only proves to be a high security of data. Thus, it achieves confidentiality of data and authenticity/ authorization for the given messages is obtained by a secured dual-check authentication based schemes proves to be a more secured and protective cloud environment , it is eventually proven by the asymmetric key Cryptography algorithms[17] depicted below such as....

Algorithm1:-

(Key-pair-creation)

1. Key pairs are (X_A, Y_A); where Priv $_{Key}$ is (X_A), P ub $_K$ey is (Y_A) and Shared $_S$ecret key is K.
2. Private Key (X_A) is signed => X_A(S). Where X_A(S) is digitally signed private key, ==> X_A (DC), where X_A (DC) is digitalcertificate issued by KDA of AS present in KDC and finally X_A (D) is digital $_I$d is generated for that private key.

3. Thus K = (X_A, Y_A, $X_A(S)$, X_A (DC), X_A (D^H)).

Algorithm2:-

(Key-process-and-manage)

1.K = { (X_A , Y_A), $X_A(S)$, $X_A(DC)$ }=> $X_A(D)^h$, where K is shared secret key b/w sender Alice(A) and ReceiverBob (B).

2. Now Alice A, has ={ K, [(X_A , Y_A), ($X_A(S)$, $X_A(D)^h$)]]}.where $X_A(S)$ is authenticated/authorized and digitally signed, $X_A(D)^h$ is digital $_I$d generated for the given msg endorsed in and it is stored in hashed format.

3. Bob B possess, such as B has = {K, [(Y_A)] } , where (Y_A) is a public key who can send any no.of messages to Alice.

4. Now Bob wants to decrypt his own message, needs private key of Alice (owner), such as B has = {A, (K, [(Y_A), (X_A)]).

5. Bob still needs digital $_I$d of private key to decrypt it finally, such as B has = {A, (K, [(Y_A), (X_A))]), $X_A(D)^h$) }.

Algorithm3:-

(Key-process-Authenticity-and-compute)

1. H (F) = {M, K ((X_A, Y_A), [$X_A(S)$, $X_A(DC)$] => X_A $(D)^h$)}.

2.=> H (F) = {M, K ([(X_A, Y_A), $X_A(S)$] , [(X_A , Y_A), $X_A(D)^h$)] }.

3. H'= {K, ([X_A, X_A $(D)^h$]), m} = M, to get the plain text message.

The particular hash function H (F) that binds or maps data of arbitrary size to data of fixed size. The values returned by a hash function are also called as hash values, hash codes, hash sums, or simply hashes.

I.e. H (F) =>$h^{'}$ = M.

I. Results and Sensitivity Analysis

Equation (1) is as follows…..

$$P = \left(n * \left[\left(\sum_{I=1}^{K} * D_S \right) * \left(\sum_{I=1}^{K} * D^h \right) \right] * (N)^K \right).$$

Where n is no.of trials, P is probability of outcomes, K is shared secret key, D_s is digital signature for that particular message, D_Id is digital Id for the given message endorsed in and stored in std. hashed way, N is no.of possible combinations based on the Key size to draw the contents present in original message.

Assume n=10 trials, D_s = message size digest is 1024 g bytes, $D_{(}$id)^h is digital Id for the message endorsed in hashed format, N=100 possible combinations, K=512 k bytes of key size length, P= probability of outcomes to decrypt the original message.

Equation (2) is as follows…..

$$P = \left(10 * \left[\left(\sum_{I=1}^{k=512} * (D_S) * 1024 \right) * \left(\sum_{I=1}^{k=512} * (D^h) * 1024 \right) * (100)^{k = 512)} \right] \right) = \infty.$$

Message digest is also a cryptographic hash function contains a string of digits created by a one-way hashing formula.Message digests are designed to protect the integrity of a piece of data or media to detect changes or alterations to any part of a message.Basically cryptographic hash function uses mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash function) that is designed to be a one-way function, and hence the function is infeasible to invert it and compute it.

II. CONCLUSION

Even for the large outcomes of data such as in 3DES standards also, the decryption of those messages takes a longer time due to it is mainly stored in secured hashed formats to the given messages in binary bit

sequences. Even if the key size is small and it is known, the intruder can't decrypt those message because it is highly secured in hashed sequences for those messages and along by the digital ID's created for the given messages. In case of DDOS (Distributed denial of service attacks) also, the intruder can't decrypt the original message, because computation of those messages even takes a longer time due to it is in secured hashed formats thus the key is secured and it is relocked again even after also many chosen messages attacks on it, thus the data is highly secured in a cloud environment in the use of protected cloud iCare.

III. FUTUREWORK

In future by use of Digital Id's/Digital signatures and digital certificates even in ISaaS (Integrated Software as a service) cloud environment also can be better and efficient secured protective cloud environment .where each user has their own username and password to store their data and uses those services by specialized apps designed by cloud vendors. Thus, it can be accessed from anywhere in the cloud by use of ICE(Integrated Cloud Environment).Even ICE poses to many attacks on the data such as by MIM attacks, DDOS attacks on it. And to protect those data vulnerabilities happening in cloud of such on-premises eco-systems by the hackers. And to protect the misuse of data happening in such on-premises can be resolved by use of Digital signatures/ Digital Id's stored in hashed standards .Thus, the impact of data vulnerabilities can be reduced and be secured to a level of extent by taken in to such level of things as possible and to be fully implemented also. So, that the known users can only use those services by in a protected cloud environment with use of protected iCare Cloud [18] in future directions and necessities.

REFERENCES

[1] Gartner. "Assessing the security risks of cloud computing", Gartner, 2008.
[2] "EHR Definition, Attributes and Essential Requirements" (PDF). Health-care Information and Management Systems Society. 2003. Archived from the original (PDF) on 19 May 2006. Retrieved 28 July 2006.
[3] "HIPAA Basics: Medical Privacy in the Electronic Age from the Privacy Rights Clearinghouse www.privacyrights.org "
[4] "HealthVault. Available from: https://www.healthvault.com."
[5] PrashantSrivastava, Satyam Singh, Ashwin Alfred Pinto, Shve-tankVerma, Vijay K. Chaurasiya and Rahul Gupta, " An architecture based on proactive IEEE,pp. 661-667.,2011
[6] S. Hameetha Begum,T. Sheeba,S. N.Nisha Rani, "Survey on cloud computing ",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1,pp 18-22, January 2013.
[7] D. Lekkas, "Establishing and managing trust within the public key infrastructure Computer Communications", 26 (16) (2003) ".
[8] Cloud Security Alliance. Top threats to cloud computing, Cloud Security Alliance, 2010."
[9] D. Polemi," Trusted third party services for health care in Europe"
[10] S. Castell, "Code of practice and management guidelines for trusted third party services", INFOSEC Project Report S2101/02, 1993.
[11] C.P. Pfleeger, S.L. Pfleeger "Security in Computing" Prentice Hall (2002).
[12] Commission of the European Community. Green paper on the security of information systems, ver. 4.2.1, 1994.
[13] D. Lekkas, S. Gritzalis, S. Katsikas "Quality assured trusted third parties for deploying secure Internet-based healthcare applications" International Journal of Medical Informatics (2002).
[14] Cloud Identity Summit, Secure the cloud now, Cloud identity summit, retrieved on 10/11/2010 from:" http:// www.cloudidentitysummit.com/."
[15] Randy Chow, Theodore Johnson and Addison-Wesley, "Distributed Operating Systems and Algorithms" 1997.
[16] http://web.mit.edu/Kerberos/, 2007/10
[17] Ayushi," A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications,ISSN: 0975 8887, Vol. 1, No. 15, 2010
[18] "Care Cloud.[cited 2013]. Available from: http://www.carecloud.de/."
[19] "Electronic Health Records Overview"(PDF). Archived from the original (PDF) on 29 December 2009." "What is a personal health record?". HealthIT.gov. Office of the National Coordinator for Health IT. Retrieved 2015-07-24.
[20] "Electronic Health Records Overview" (PDF). Archived from the original (PDF) on 29 December 2009.
[21] Ferguson, Niels; Schneier, Bruce (2003). Practical Cryptography. Wiley. ISBN 0-471-22357-3.
[22] Katz, Jon; Lindell, Y. (2007).'' Introduction to Modern Cryptography." CRC Press.ISBN 1-58488-551-3.
[23] Menezes, A. J.; van Oorschot, P. C.; Vanstone, Scott A. (1997). Handbook of Applied Cryptography.ISBN 0-8493-8523-7.
[24] IEEE 1363:'Standard Specifications for Public-Key Cryptography" Christof Paar, Jan Pelzl," Introduction to Public-Key Cryptography", Chapter 6 of "Understanding

[25] Cryptography, A Textbook for Students and Practitioners". (Comparison web site contains online cryptography course that covers public-key cryptography), Springer, 2009.
[26] Blakley, G. R. (1979). "Safeguarding cryptographic keys". Proceedings of the National Computer Conference 48: 313317.
[27] Yu, S. et al. ''Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing." IEEE INFOCOM 2010.
[28] Turner, Dawn M. "What Is Key Management? A CISO Perspective". Cryptomathic. Retrieved 30 May 2016.
[29] Barker, Elaine; Smid, Miles; Branstad, Dennis; Chokhani, Santosh. "NIST Special Publication 800 -130: A Framework for Designing Crypto-graphic Key Management Systems" (PDF).National Institute of Standards and Technology. Retrieved 30 May 2016.
[30] " Key Management Solutions by Safe Net: Protect and Manage Crypto-graphic Keys". Safenet-inc.com. Retrieved 2013-08-06.
[31] "Key Management: key Authority - a proven solution for centralizing key management". Thales-esecurity.com. Retrieved 2013-08-06.
[32] "Encryption Key Management — Encryption Key Management, Cloud Security, Data Protection". Townsendsecurity.com. Retrieved 2013-08-06.