Journal of Engineering and Applied Sciences 14 (15): 5250-5257, 2019
ISSN: 1816-949X

Data Security between Challenges and Solutions: Cryptography as a Solution in Cloud Computing

Nancy Awadallah Awad
Department of Computer and Information Systems, Sadat Academy for Management Sciences, Cairo, Egypt
rarecore2002@yahoo.com 01003681828

Abstract: The benefits of cloud storage which are cost efficiency, resilience, scalability and data high reliability, due to that all data firms is moving to the cloud that are easy to access from anyplace, anyhow, anytime. Therefore, the need to protect data has become a necessity against denial of services, unauthorized users and access. The security and trust issues are still challenges in cloud computing field which should be solved, secure the storage databases hosted by the cloud provider, the user's data has to be released to the cloud and thus, leaves the protection-sphere of the data owner. This study focuses on various threats which are considered challenges for cloud computing and presents cryptography as a data security solution in cloud computing. Also, this study presents a framework of a hybrid cryptography algorithm through using DES and RSA for encryption and decryption phases sequentially.

Key words: Cloud computing, data protection, cloud service provider, cryptography, DES, RSA

INTRODUCTION

Cloud computing refers to applications and services that run on a distributed network using virtualized resources provisioned as a service over the internet accessed by common internet protocols and networking standards (Jensen *et al*., 2009). The "cloud" term refers to the two concepts abstraction and virtualization. The meaning of abstraction is that system implementation is abstracted by cloud computing. Where the meaning of virtualization is that systems are virtualized by pooling and sharing resources (Sosinsky, 2011). The access technologies can vary from service enabled fat clients to web browser-based thin clients based on type of cloud such as Infrastructure as as Service (IaaS), Platform as as Service (PaaS) and Software as as Service (SaaS) (Jensen *et al*., 2009). Web services security defines how to provide integrity, confidentiality and authentication for SOAP messages.

Cloud computing has several benefits cause of its characteristics such as resource pooling, rapid flexibility and access on-demand administration and measured services (Timothy and Santra, 2017). Despite of the previous benefits there are challenges and disadvantages of cloud computing. To face the problem of data security issues in cloud computing, several challenges are introduced. In cloud computing, different security issues are applied one solution for data security and integrity problem is encryption.

Cloud services and deployment models: Definitions that separate cloud computing into service models and deployment models are set by the US National Institute of Standards and Technology (NIST) (Sosinsky, 2011). Those models and their relationship to essential characteristics of cloud computing are shown in Fig. 1. Two distinct sets of models of cloud computing are classified into:

Deployment models: Which refers to the cloud's infrastructure location and management.

Service models: Which consists of services types that user can access on a cloud computing. Table 1 illustrates types of cloud models. Researcher's classified cloud computing deployment models as follows.

Public cloud: Is available for public use for a large industry group and is owned by an organization selling cloud services.

Private cloud: Is operated for the exclusive use of an organization, the cloud may be managed by that organization. Private clouds may be either on- or off-premises.

Community cloud: It may be managed by the organization it is one where the cloud has been organized to serve a common function.

Hybrid cloud: Combines multiple clouds (private, community of public). It may offer standardized or proprietary access to data and applications.

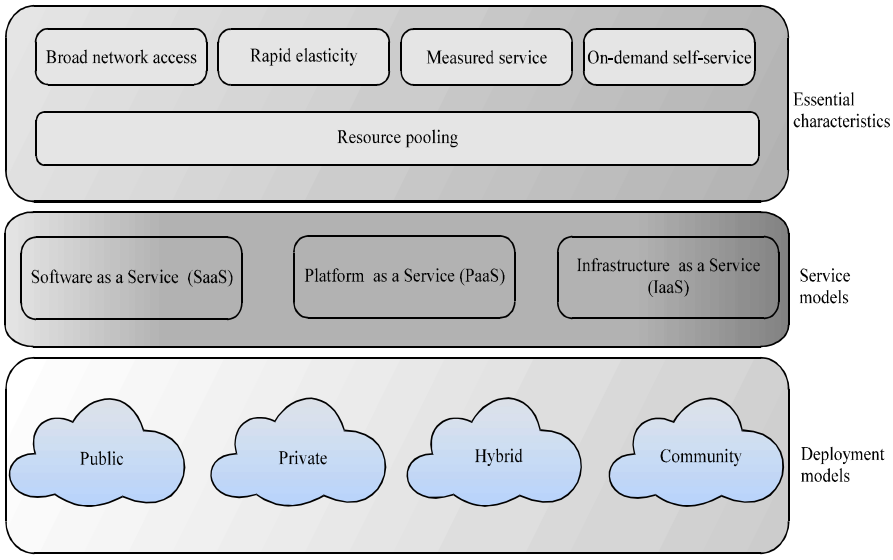

Fig. 1: The NIST cloud computing definitions

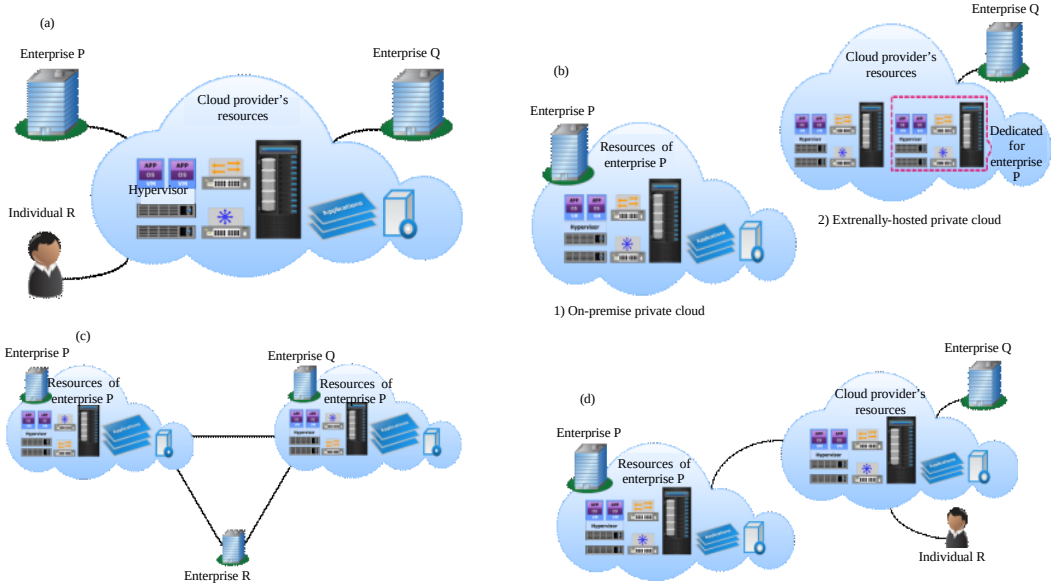

Fig. 2: Four deployment models of cloud computing: a) Public cloud; b) Private clouds; c) Community cloud and d) Hybrid cloud

Table 1: Cloud service models

Cloud services	Service	Customers	Examples
Infrastructure as a Service (IaaS)	Customer can store data in the cloud	Enterprise and developers	MS Azure storage, Amazon S3
Platform as a Service (PaaS)	Customer can run its apps in the cloud	Developers	MS Azure, Amazon EC2, Google AppEngine
Software as a Service (SaaS)	Customer makes use of app in the cloud	Consumers and enterprise	Web-based email, Facebook, Office Web, Google Docs

Literature review

Security challenges of cloud computing: This study presents previous studies which discussed cloud computing security issues. Each issue is termed and its impact is described. Table 2 illustrates challenges issues of cloud computing security.

Data security classification: Data has 3 states which are varied in time between generation stages to destroy stage. Figure 2 and 3 illustrates the representation of data security classification. Cross-cutting is considered security issue that can be raised through any or all of the states (Kumar *et al*., 2017). Data in

Table 2: Challenges of cloud computing security

Security issues	Descriptions
XML signature	XML signature Element Wrapping is a well-known type of attacks on protocols using XML Signature for authentication or integrity protection (McIntosh and Austel, 2005; Rahaman *et al.*, 2006)
Browser security	Attacks on browser-based cloud authentication: the browser itself is unable to generate cryptographically valid XML tokens to authenticate against the cloud, this is done with the help of a trusted third party. For example, Microsoft's passport (Kormann and Rubin, 2000)
Cloud integrity and binding	The role of cloud system is to determine the address for accessing that new instance is to be communicated back to the requesting user. This task is implemented by requiring metadata on the service implementation modules at least for identification purposes (Bellwood *et al.*, 2004)
Flooding attacks	Attacker sending requests to servers to be flood which be a threat. This is represented in Denial of Service (DoS) threat (Jensen and Gruschka, 2008)
Cloud Service Provider (CSP) Level attacks	Sharing resources are examples of CSP which may be attacked as next: SQL injection Side channel Malicious Insider Guest-hopping (Kuyoro, 2011; Ukil *et al.*, 2013)
Network level security attack	A trial of user wants to attack the cloud for any purpose, attacks may be represented as: Domain Name System (DNS) attacks Domain hijacking IP Spoofing (Kandukuri and Rakshit, 2009)
End user's attacks	It can be any process of software vulnerabilities such as phishing, fraud which can threaten the cloud service infrastructure (Plossl *et al.*, 2005)
Data integrity and location	It represented in cloud user's personal data security threat at the same time without knowing the data storage location (Teneyuca, 2011; Ryan and Falvey, 2012) because Data owners have no physical control over their data (Yu *et al.*, 2012)
Access control and authentication	Encryption considered an issue of security concerns for cloud computing as it related to safe computing from unauthorized access and unauthorized users (Ahmed and Hossain, 2014; Kumar *et al.*, 2017). Therefore, data owner should be informed at the same time when the process of verification validation are performed on the modifications and deletions for any data in the cloud computing (Boneh *et al.*, 2011)
Trust	It is important to use cloud service as it has the authenticity and credibility of the CSP. To gain trust model is important issue in cloud computing (Abbadi and Martin, 2011)

Table 3: Data states

Data states	Descriptions
Data at rest	It means data stored on persistent storage devices on a cloud
Data in use	It means data in processing, it can be held in s RAM and cache memory
Data in transit	It means data in motion, it may be moving from local storage to the cloud service provider's cloud storage
Cross-cutting issues	Cross cutting attack as a result of virtual machine's network information leakage (Ristenpart *et al.*, 2009). The de-duplication in cloud storage is the main reason of information leakage (Mulazzani *et al.*, 2011; Harnik *et al.*, 2010) while research (Squicciarini *et al.*, 2010) referred the cause to the indexing in clouds

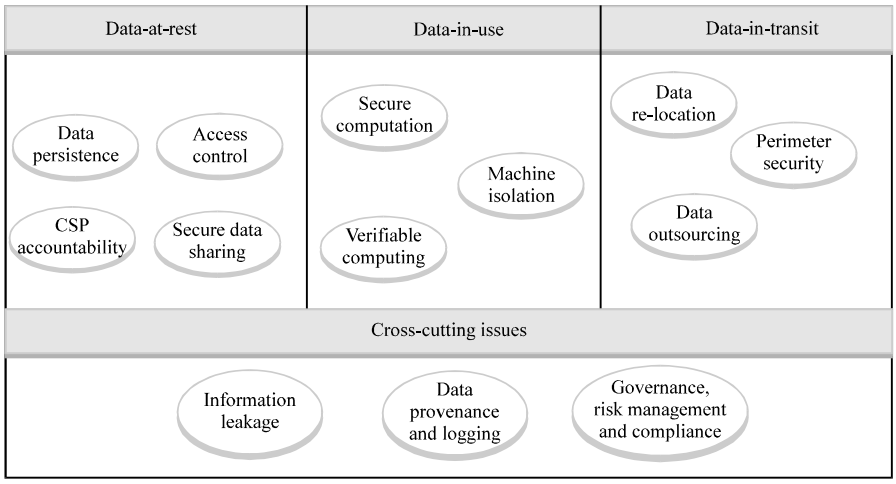

Fig. 3: Data security classification (Kumar *et al.*, 2017)

transit at rest, backup media should be encrypted by secure key store which protect encryption keys. Table 3 describes the classification of data states.

MATERIALS AND METHODS

Security solutions of cloud computing: To obtain the confidentiality and trust, access control, data encryption

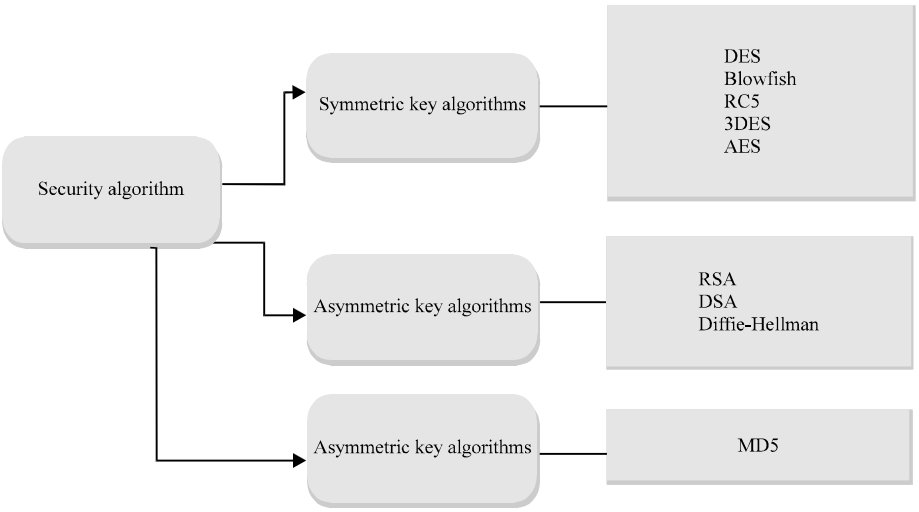

Fig. 4: Cryptography algorithms

and cryptographic processors can be used (Tan *et al*., 2013, 2015). Cloud Service Provider (CSP) such as Microsoft Azure and Amazon Web Services, allowing the user easy to access at any time and everywhere in the world (Ko, 2010; Scoon and Ko, 2016). Therefore, cryptography is a way to protect data in cloud computing from any unauthorized usage. It means encoding a meaningful data and the sender decode it. This study discusses the types of cryptography and its methods.

Cryptography: Cryptography can help cloud computing when make storage data more secure, safe and data confidentiality and this achieved on the cloud when data is encrypted. But the problem of data to be vulnerable to attacks arise cause of decryption process which be done before being processed. Therefore, the need for data encryption will be necessary which and achieving confidentiality in the cloud and increasing user's trust. Cryptography can solve the problems related to data security in cloud computing such as backup data, network traffic, file storage system and security of host.

Encryption prevent others problems such as session hijacking, spoofed attacks and man-in-the-middle. There are new challenges in cloud computing security as data manipulation without being trusted (Boneh *et al*., 2011).

For overcoming the above problems, cryptography has been applied to ensure data security, privacy and trust in cloud computing. Figure 4 illustrates the classification of cryptography algorithms.

Symmetric key algorithms: Symmetric uses single key which works for both encryption and decryption. The symmetric systems provide a two channel system to their users.

Data Encryption Standard (DES): Triple-DES and Advanced Encryption Standard (AES) are the most symmetric-key algorithms used in cloud computing. Stream cipher one bit is encrypted at a particular time. Figure 5 illustrates encryption and decryption of DES methods as an example of symmetric key.

Asymmetric key algorithms: In this algorithm different keys are used for encryption and decryption. Each receiver possesses a decryption key of its own, referred to as his private key. Examples of Asymmetric key are Rivest-Shamir-Adelman Encryption (RSA) cryptosystem and Diffie-Hellman key exchange. RSA algorithm is an asymmetric encryption algorithm. There are two keys used in RSA D and E. Which can be used interchangeably but one must be kept private and another becomes public. A user1 which wants to share data with user 2 must encrypt his message with user 2's public key which only the second user can decrypt with user 2 private key. The E and D can be viewed as a complimentary function which can be applied in any order:

$$P = E\left(D\left(P\right)\right) = D\left(E\left(P\right)\right)$$

A plain text block is encrypted as P^e mod n. Factoring P^e to uncover the plain text is difficult, since, exponentiation is performed mod n. The receiver who knows the decrypting key d can easily retrieve P by computing (P^e) d mod n. Figure 6 is an example of using RSA method to encrypt and decrypt message.

Hashing algorithms: It is a mathematical algorithm that represents data of despotic size to a hash of a fixed size. It's a one-way function, infeasible to invert. Message-Digest algorithm-(MD5) is an example of hash

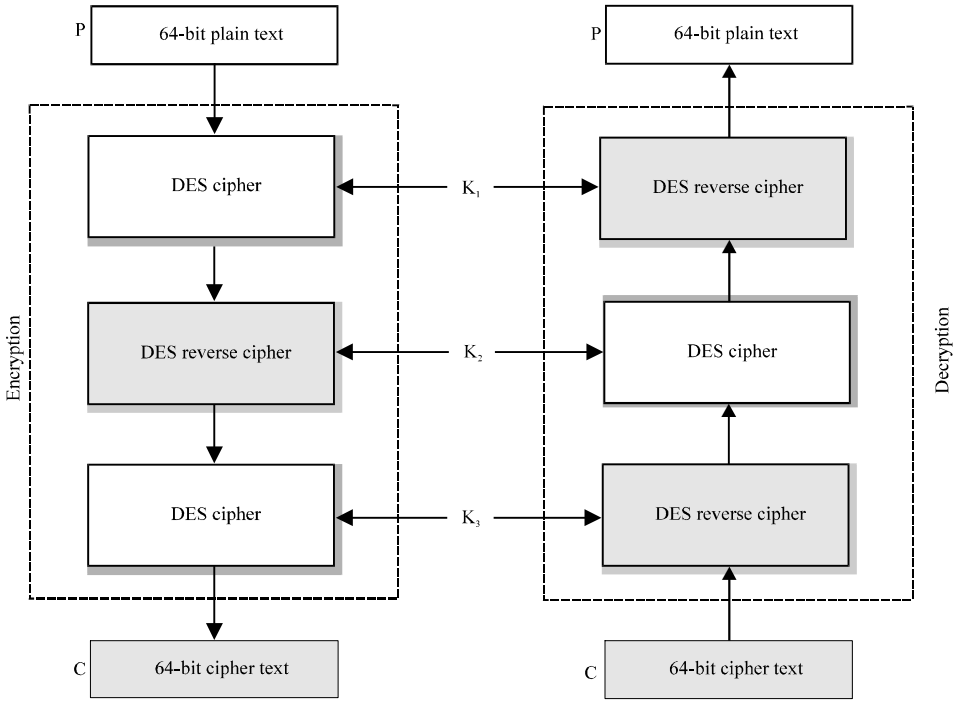

Fig. 5: Data Encryption Standard (DES) methods

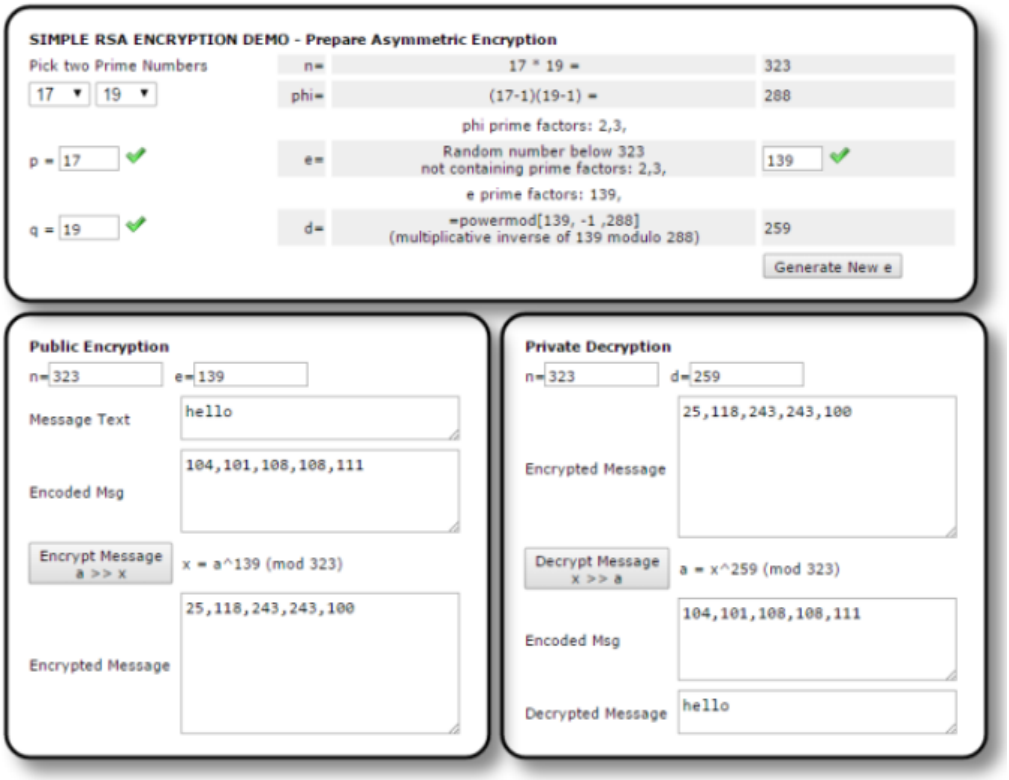

Fig. 6: Simple RSA encryption and decryption message

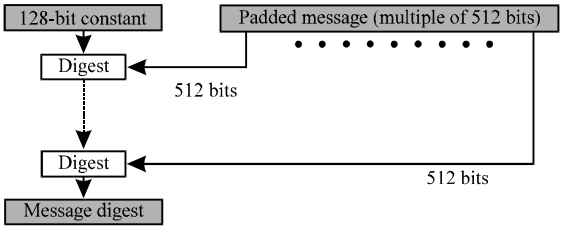

Fig. 7: MD5 block diagram

function algorithm in cryptography it is used for achieving data integrity. To encrypt the message the data sender uses the public key and to decrypt the message the receiver uses its private key (Chatterjee *et al*., 2017). Figure 7 illustrates MD5 block diagram as an example of hashing algorithm. Cryptographic algorithms achieved benefits for cloud storage security are:

- The data is encrypted on the data processors which due to that users can be trusted that the privacy of their data is saved
- A cryptographic storage service data is only stored in encrypted form

RESULTS AND DISCUSSION

Proposed framework: Researcher in this study proposed a framework that presents a hybrid cryptography method by using two key algorithms one for encryption phase and other one for decryption phase. Researcher proposed using DES as an example of symmetric key and its role in this framework to encrypt plaintext and for decrypted this data RSA algorithm will be used as an example of asymmetric key. Cryptography algorithm consists of the encryption and decryption phases. In encryption phase the plaintext is transformed into cipher data (scrambled data). Decryption phase is used to get the plaintext from cipher data.

Encryption phase: In this phase converts the plaintext into cipher data by secret key via. using DES algorithm (symmetric key) cryptography method and send this key with encrypted data to the receiver. The role of encryption process is to protect data from unauthorized user or access in cloud.

Decryption phase: In this phase cipher data is converted into plaintext again via. using RSA algorithm (Asymmetric key) cryptography method. Figure 8 illustrates the proposed framework of cryptography algorithm.

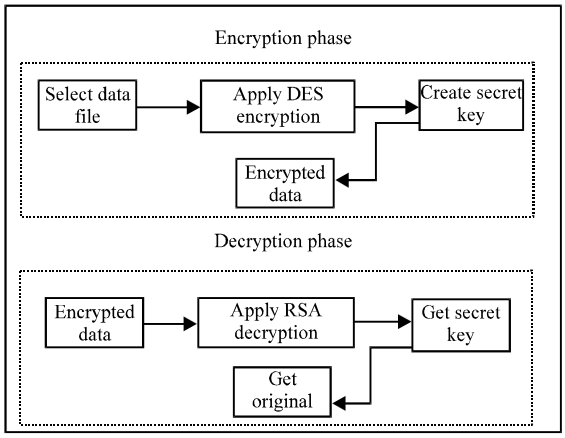

Fig. 8: Proposed framework for hybrid cryptography algorithm

CONCLUSION

Data security still one of the most concerns issues of the cloud computing. Cryptography can be used for maintaining cloud data access control, cloud data trust management, verifiable computing, cloud data authorization and authentication and secure data storage. DES, RSA, MD5 are most popular secure algorithms which service providers use for secure communication and storage of data. In this study, the framework hybrid cryptography algorithm is proposed via. using DES symmetric key for encryption phase and RSA asymmetric key for decryption phase.

ACKNOWLEDGEMENT

I woud like to thank everyone help me to prepare this paper.

REFERENCES

Abbadi, I.M. and A. Martin, 2011. Trust in the cloud [Elektronische versie]. Inform. Security Tech. Rep., 16: 108-114.

Ahmed, M. and M.A. Hossain, 2014. Cloud computing and security issues in the cloud. Int. J. Network Secur. Applic., 6: 25-36.

Bellwood, T., S. Capell, L. Clement, J. Colgrave and M.J. Dovey *et al*., 2004. UDDI Version 3.0.2. UDDI Spec Technical Committee Draft, OASIS, Billerica, MA., USA.

Boneh, D., A. Sahai and B. Waters, 2011. Functional encryption: Definitions and challenges. Proceedings of the International Conference on Theory of Cryptography, March 28-30, 2011, Springer, Berlin, Germany, ISBN:978-3-642-19570-9, pp: 253-273.

Chatterjee, R., S. Roy and U.G. Scholar, 2017. Cryptography in cloud computing: A basic approach to ensure security in cloud. Intl. J. Eng. Sci., 7: 11818-11821.

Harnik, D., B. Pinkas and A. Shulman-Peleg, 2010. Side channels in cloud services: Deduplication in cloud storage. IEEE Secur. Privacy, 8: 40-47.

Jensen, M. and N. Gruschka, 2008. Flooding attack issues of web services and service-oriented architectures. Proceedings of the International Workshop on Security for Web Services and Service-Oriented Architectures (SWSOA), September 8-13, 2008, Munich, Germany, pp: 117-122.

Jensen, M., J. Schwenk, N. Gruschka and L.L. Iacono, 2009. On technical security issues in cloud computing. Proceedings of the IEEE Conference on Cloud Computing ICCC, September 21-25, 2009, IEEE, Bangalore, India, ISBN:978-1-4244-5199-9, pp: 109-116.

Kandukuri, B.R. and A. Rakshit, 2009. Cloud security issues. Proceedings of the IEEE International Conference on Services Computing (SCC'09), September 21-25, 2009, IEEE, Bangalore, India, ISBN:978-1-4244-5183-8, pp: 517-520.

Ko, R.K., 2010. Cloud computing in plain English. XRDS., 16: 5-6.

Kormann, D.P. and A.D. Rubin, 2000. Risks of the passport single signon protocol. Comput. Networks, 33: 51-58.

Kumar, V., S. Chasiri and R. Ko, 2017. A Data-Centric View of Cloud Security. In: Data Security in Cloud Computing, Kumar, V., S. Chaisiri and R. Ko (Eds.). The Institution of Engineering and Technology, Michael Faraday House, Stevenage, ISBN: 9781785612206, pp: 1-13.

Kuyoro, S., 2011. Cloud computing security issues and challenges. Int. J. Comput. Networks, 3: 247-255.

McIntosh, M. and P. Austel, 2005. XML signature element wrapping attacks and countermeasures. Proceedings of the 2nd ACM Workshop on Secure Web Services, Fairfax, VA, USA., November 11, 2005, ACM, New York, USA., pp: 20-27.

Mulazzani, M., S. Schrittwieser, M. Leithner, M. Huber and E. Weippl, 2011. Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space. Proceedings of the 20th USENIX Symposium on Security, August 10-12, 2011, San Francisco, California, USA., pp: 65-76.

Plossl, K., H. Federrath and T. Nowey, 2005. Protection mechanisms against phishing attacks. Proceedings of the International Conference on Trust, Privacy and Security in Digital Business, August 22-26, 2005, Springer, Berlin, Germany, ISBN:978-3-540-28224-2, pp: 20-29.

Rahaman, M.A., A. Schaad and M. Rits, 2006. Towards secure SOAP message exchange in a SOA. Proceedings of the 3rd ACM Workshop On Secure Web Services, Alexandria, VA, USA., November 3, 2006, ACM, New York, USA., pp: 77-84.

Ristenpart, T., E. Tromer, H. Shacham and S. Savage, 2009. Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. Proceedings of the 16th ACM International Conference on Computer and Communications Security (CCS '09), November 9-13, 2009, ACM, Chicago, Illinois, USA., ISBN:978-1-60558-894-0, pp: 199-212.

Ryan, P. and S. Falvey, 2012. Trust in the clouds. Comput. Law Security Rev., 28 : 513-521.

Scoon, C. and R.K. Ko, 2016. The data privacy matrix project: Towards a global alignment of data privacy laws. Proceedings of the 2016 IEEE International Conference on Trustcom/BigDataSE/ISPA, August 23-26, 2016, IEEE, Tianjin, China, pp: 1998-2005.

Sosinsky, B., 2011. Understanding Cloud Architecture. In: Cloud Computing Bible, Sosinsky, B.A. (Ed.). John Wiley & Sons, ýHoboken, New Jersey, USA., ISBN:9788126529803, pp: 45-65.

Squicciarini, A., S. Sundareswaran and D. Lin, 2010. Preventing information leakage from indexing in the cloud. Proceeding of the 3rd International IEEE Conference on Cloud Computing, July 5-10, 2010, IEEE, Miami, Florida, ISBN: 978-1-4244-8207-8, pp: 188-195.

Tan, A.Y.S., R.K.L. Ko, G. Holmes and B. Rogers, 2015. Provenance for Cloud Data Accountability. In: The Cloud Security Ecosystem: Technical, Legal, Business and Management Issues, Ko, R. and R. Choo (Eds.). Elsevier, ýAmsterdam, Netherlands, ISBN:9780128017807, pp: 171-185.

Tan, Y.S., R.K. Ko and G. Holmes, 2013. Security and data accountability in distributed systems: A provenance survey. Proceedings of the 2013 IEEE 10th Joint International Conference on High Performance Computing and Communications and Embedded and Ubiquitous Computing, November 13-15, 2013, IEEE, Zhangjiajie, China, pp: 1571-1578.

Teneyuca, D., 2011. Internet cloud security: The illusion of inclusion. Inf. Secur. Tech. Rep., 16: 102-107.

Timothy, D.P. and A.K. Santra, 2017. A hybrid cryptography algorithm for cloud computing security. Proceedings of the 2017 International Conference on Microelectronic Devices, Circuits and Systems (ICMDCS), August 10-12, 2017, IEEE, Vellore, India, ISBN:978-1-5386-1717-5, pp: 1-5.

Ukil, A., D. Jana and A. De Sarkar, 2013. A security framework in cloud computing infrastructure. Intl. J. Netw. Secur. Appl., 5: 11-24.

Yu, S., W. Lou and K. Ren, 2012. Data Security in Cloud Computing. In: Handbook on Securing Cyber-Physical Critical Infrastructure, Das, S.K., K. Kant and N. Zhang (Eds.). Elsevie, Amsterdam, Netherlands, ISBN:9780124159105, pp: 392-409.