ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/261201256

Use of cryptography in cloud computing

Conference Paper · November 2013

DOI: 10.1109/ICCSCE.2013.6719955

CITATIONS
64

READS
20,423

2 authors:

Aws Jaber
KTH Royal Institute of Technology
60 PUBLICATIONS **485** CITATIONS
SEE PROFILE

Mohamad Fadli Zolkipli
Northern University of Malaysia
73 PUBLICATIONS **1,546** CITATIONS
SEE PROFILE

All content following this page was uploaded by Aws Jaber on 17 May 2016.

The user has requested enhancement of the downloaded file.

Use of Cryptography in Cloud Computing

Aws Naser Jaber[1]
Faculty of Computer Systems & Software Engineering
Universiti Malaysia Pahang
Kuantan, Malaysia
aws_z2010@yahoo.com

Mohamad Fadli Bin Zolkipli[2]
Faculty of Computer Systems & Software Engineering
Universiti Malaysia Pahang
Kuantan, Malaysia
fadli@ump.edu.my

***Abstract*—Cloud computing is a platform for expanding capabilities and developing potentialities dynamically without employing new infrastructure, personnel, or software systems. In Addition, cloud computing originated from a commercial enterprise concept, and developed into a flourishing IT invention. However, given that considerable information on individuals and companies are identified in the cloud, concerns have been raised regarding the safety of the cloud environment. Despite the hype surrounding cloud computing, customers remain reluctant to deploy their commercial enterprise into the cloud. Nevertheless, lack of protection is the only major concern that hinders increased use of cloud computing. Furthermore, the complexity with which cloud computing manages data secrecy, and information security makes the market hesitant about cloud computing. The architecture of cloud models threatens the security of existing technologies when deployed in a cloud environment. Thus, users of cloud services should know the dangers of uploading data into this new environment. Therefore, in this paper different cryptography aspects that pose a threat to cloud computing are reviewed. This paper is a survey of specific security issues brought by the use of cryptography in a cloud computing system.**

***Index Terms*— Cloud encryption, cryptographic algorithms, cloud security infrastructure.**

I. Introduction

Depend about it, and the terminology and concepts associated with it provide significant insight. Literature on cloud computing has blurred the real meaning of cloud computing. However, several companies make their service needs at the term "cloud computing" originates from network topology. A conventional cloud is shown in Fig. 1. Cloud computing refers to the conduct of practical applications or services in an Internet [1]. Cloud computing did not rapidly emerge; it may be traced back in some form to when computing systems had computing resources ,and practical applications that were remotely time-shared. Concerns have been raised regarding the different varieties of applications and their services fetched by clouds. In numerous cases, the devices and applications used in these services involve no extraordinary function. Many companies avail of services from the cloud. As in 2010, an instance of companies availing of cloud computing services produced the following: Microsoft has the Microsoft® SharePoint® online service, which allows content and business enterprise intelligence tools to be uploaded into the cloud and makes office practical applications available in the cloud. Google cloud storage delivering many services for formal users, and large infrastructure I.T companies [2]. In addition, Salesforce.com made their own cloud services for its customers [3]. Further, Vmforce, and other paid services aloes grown-up in cloud services nowadays [4]. However, maybe till yet the cloud clue not clear, and a question may be given what, and why cloud computing exactly? Whose care has cloud platform, and what about the security, and encryption. The following sections try to give a clear idea about service models z, characteristics, deployment models, advantages, and cryptography features with cloud computing.

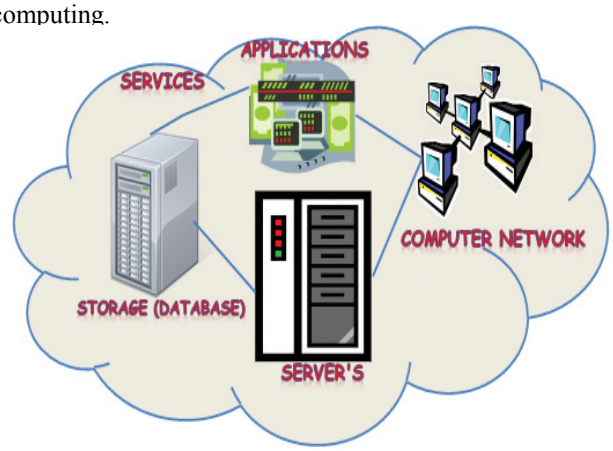

Fig. 1. Cloud computing

II. Cloud Computing Features

Cloud computing has various features, the most important of which are as follows:

1. Distributed Infrastructure: Cloud computing has a virtualized software framework, for example, networking capabilities, and optionally shared physical services. More further, cloud computing can also be used for storage. The cloud infrastructure, regardless of the deployment model, builds visible infrastructure according to the identified number of users.

2. Dynamic Provisioning: Services for actual necessity are automatically permitted through software automation. The elaboration and compression of service capacity is optional. These dynamic scaling demands are targeted while maintaining high reliability and protection.
3. Network Access: An Internet connection is required to achieve an across-the-board access to devices, such as PCs, laptops, and mobile devices, by using standard-based API representatives established on HTTP. Deployments using cloud services include practical business applications to cutting-edge applications in the latest smart phones.
4. Managed Metering: A meter for managing and optimizing service and for supplying reporting and billing data is used in cloud computing. Cloud computing provides multiple sharing and scalable services as necessary from almost any location. The consumer is charged for these services on the basis of actual usage.

III. SERVICE MODELS

When cloud computing was first created, the services it offered were deployed in business conditions with high demands as shown in Fig.2. Common service examples include:

• Software as a Service (SaaS): Consumers buy the ability to access and use an application or service hosted in the cloud [5]. Microsoft is increasing its involvement in this area. As a part of the cloud computing option for Microsoft Office 2010, Microsoft's Office Web Apps are accessible to Office volume licensing customers and Office Web App subscribers through its cloud-based online services.
• Platform as a Service (PaaS): Consumers purchase access to platforms to deploy their own software and applications into the cloud [6]. Consumers do not manage the operating systems and network access, and constraints may be placed on which applications can be deployed.
• Infrastructure as a Service (IaaS): Consumers control and manage system processes, applications, storage, and network connectivity [7] and do not merely maintain the cloud infrastructure. In addition, the various subsets of these cloud models in an industry or market are recognized. Communications as a Service (CaaS) is one such subset model used to distinguish hosted IP telephony services. CaaS caused a shift to additional IP-centric communications and numerous Session Initiation Protocol (SIP) trunk deployments [8]. Installing IP and SIP facilitates the entry of private branch exchange(PBX) into the cloud [9]. In this case, CaaS can be considered a subset of SaaS deployment models.

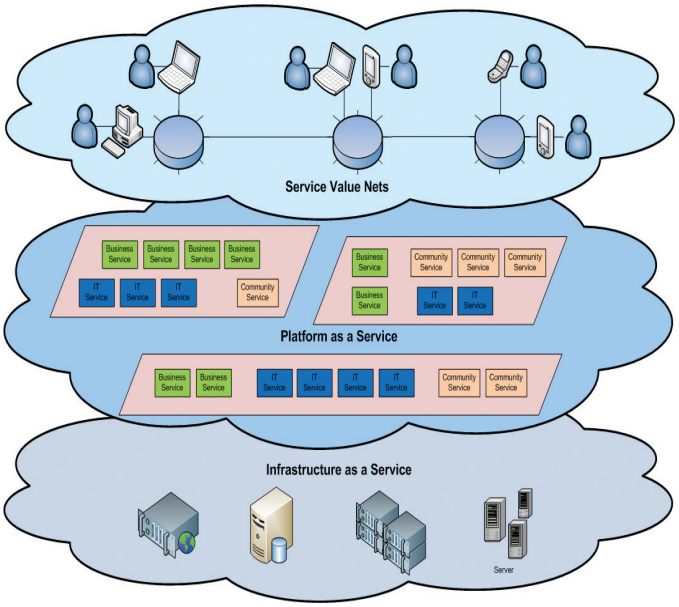

Fig.2. Service model

A. Cloud deployment models

Define Cloud computing has requirement issues; the four deployment models that can be adopted to address these issues are as follows:

1. Private Cloud: is deployed, observed, and engaged for a particular distance area. However, it will be overseas through internet connection. But from private branch-branch.
2. Public Cloud: infrastructure is available to the public users, for example, Google-Drive service. In fact, public cloud enables a consumer to develop and deploy a service in the cloud with very little financial outlay compared with the capital usually required with other cloud computing services.
3. Hybrid Cloud: Any cloud infrastructures have numerous clouds in different area. Only the clouds allow information, or partial information that allowed shifting between clouds. Private and public clouds can be compounded to support the requirements of retaining organizational data and offer services in the cloud.
4. Community Cloud: This cloud is used for large infrastructure, such as government organizations that connect to one cloud to upload data with unified information or a campus server that connects one cloud computing community.

While, in Fig.3. Also shows that 35% of information technology users do not use cloud servers because of security issues. These users must be aware of other cloud computing services without security. The number of private cloud users has slowly increased because the cost of servers is based on hardware, software, and the expertise required implementing

these components. Public cloud servers make up 17% of the total number of cloud servers. Public cloud servers are free services offered through free main cloud providers, such as MSN, Yahoo, and Google. Hybrid clouds may be the most developed service in the world because the costs for mixing private, and public clouds are affordable.

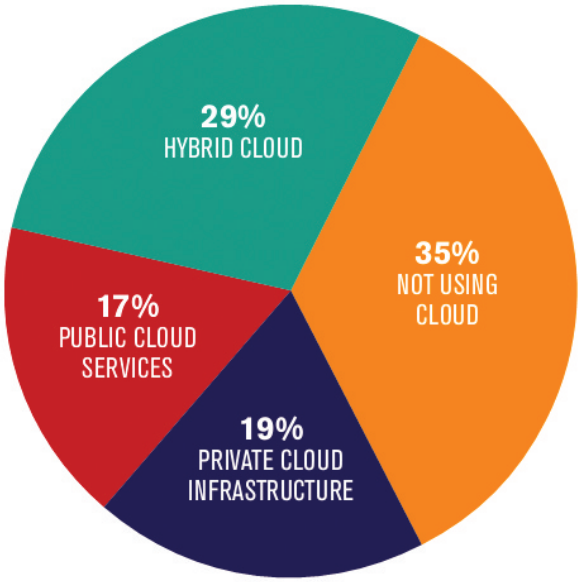

Fig.3. Cloud computing usage

As discussed above, increasing attention is paid to cloud computing attacks. These attacks may be done for several purposes, such as for gaining valuable information on large-scale organizations or forging personal information. Fig. 4 shows an example of how an attacker can penetrate a virtual machine into the hypervisor of the cloud environment.

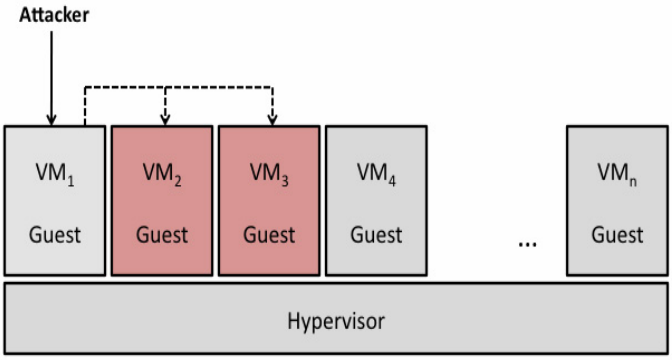

Fig.4. An example of attacking case to virtual machine

IV. Cloud Computing and Cryptographic

Cryptography involves the conversion of clear text into an unreadable form. Cryptography is a technique frequently used to transfer contents safely by ensuring that only the intended recipient can read them. This domain spotlight provides an overview of the history of cryptography and the many complex, imaginative approaches used in contemporary enterprise encryption.

A. Cloud computing encryption

Encryption for cloud computing world is an important issue that needs to investigate in several studies. One major focuses of encryption in cloud computing is identification based on encryption. An example of encryption is as follows:

Encryption: Assume E_1 and E_2 are two entities in the cloud computing. The identity of entity E_2 is $ID_{E_2} = DN_0 \| DN_1 \| DN_2$. To encrypt message m with ID_{E_2}, E_1 acts as follows:

1. Compute

$$P_1 = H_1(DN_0 \| DN_1) \quad (1)$$

$$P_2 = H_1(DN_0 \| DN_1 \| DN_2) \quad (2)$$

2. Choose a random $r \in \mathbb{Z}_q^*$;

3. Output the ciphertext

$$C = < rP, rP_1, rP_2, H_2(g^r) \oplus m > \quad (3)$$

where $g = \hat{e}(Q_0, P_0)$ which can be pre-computed.

V. Review of Studies on Cryptography for Cloud Computing

Bleikertz et al. [10] proposed the secret key principles, which are applied to virtual machines on the basis of unique client-controlled CaaS architecture for cloud computing. However, these researchers emphasized the use of physical hardware security modules, and found that architecture segregates the management and storage of the keys of cloud clients as well as all cryptographic operations into a secure crypto-domain called DomC, which is tightly coupled to the workloads of clients.

While, Sanyal and Iyer [11] investigated cloud security based on public key values. They discussed a secure, and efficient algorithm based on the multi-key encryption AES technique, a 128/192/256 bit cipher key used to encrypt and decrypt data. Results confirmed, that AES increases security for the cloud computing compared with RSA. But, AES can be used in virtual machines and in public or private clouds.

Mao [12] noted an important problem for secure network virtualization: the negligent usage of intelligence and distributed power by hypervisors. The research discussed how hypervisors use information boxes to gain control. Therefore, he proposed network virtualization using modern technology with several useful applications, including secure multi-tenancy for cloud computing. Cryptography significantly affects the management of the intelligence and distributed power of hypervisors.

Rauber [13] studied cloud computing security, which the entire system requires or else it collapses. Rauber in fact, argued that the main components of a cloud should be secure and discussed whether cloud computing will revolutionize the computing experience. The researcher also examined the functions of SaaS, homomorphic encryption, and functional encryption and their strategies for keeping information secure. These topics were discussed in depth together with useful results.

Zaheng [14] focused on the unique challenge posed by security by building an enhanced security- mobile cloud. Zaheng defined encryption data through public key cryptography such that a sender can retrieve data from a cipher text stored in the cloud without relying on the recipient of the cipher text. Privacy is a significant issue in cloud computing.

While, on Facebook, content may be shared on other social networks, such as Twitter and LinkedIn, through the Share. However, Zaheng observed that using mobile cloud computing servers when browsing social networks remains a significant security issue.

Kerchbaun [15] identified several stuck cloud security issues, such as infrequent queries, security versus performance query optimization, and access control, and developed a high-performance prototype suitable for practical adoption.

Ustimenko and Wroblewska [16] proposed a brilliant idea for homomorphic encryption and multivariate key cryptography and found that algebra is important for cryptography for cloud computing security.

Chakrborty et al. [17] proposed elliptic curve cryptography for a homomorphic encryption scheme. Initial implementation produced a high data self-control scheme. The application verified the retrievability scheme, where the client was able to challenge the integrity of the stored data. Notion is important for proposals in cryptography; thus, Chakrborty et al. have used the notions that the third party auditor is a highly secure method. However, the notion was used to verify and modify secure path data on behalf of the client. A Merkle hash tree was used for data server storage because the authors assumed that this tree securely accelerates data access.

While, in PKI, several studies have complained about the cost of elliptic curve cryptography; such high cost can be remedied only by enhancing the ECC algorithm [18]. Jangar and Bala used RSA to construct a privacy-aware security algorithm in a cloud environment and found that the algorithm is efficient, secure, and private when used in a cloud environment.

Important studies on cloud security have examined secure paths for cryptography, such as privacy and data integrity [19]. Few studies have investigated the concealment of information from clients and users. Thus, Wazed Nafi et al. proposed a secure way to construct cloud-computing platforms: an advanced AES encryption system for hiding information sessions between clients and servers. AES-based file encryption systems and asynchronous key systems for exchanging information or data are included in this model. As a result, PaaS, SaaS, and IaaS can use AES for these three cloud models to hide information against traces and packets sent to the cloud infrastructure.

Eyers and Russello [20] argued that the cloud computing trend will increasingly become challenging as the number of consumers rise. Cloud computing also has various threats to its model from self-hosted resources. In fact, cloud computing is trusted, and consumers are curious about it, even if such curiosity is unintended. F, it providers large prime keys to create secure sessions. However, this method will impair the performance of many cloud applications.

Dodis et al. [21] analyzed key-insulated symmetric key cryptography, which reduces the damage caused by looping attacks against integrated cryptographic software. They emphasized the feasibility of symmetric key cryptography in key-insulated cryptography and produced a proof-of-concept kernel-based virtual machine environment.

Sudha [22] studied cloud security for data integrity, confidentiality, and authentication through a model that uses hyper crypto-encryption for asymmetric and symmetric cryptographic algorithms as a part of a security model for data security in cloud computing.

Gampala et al. [23] explored data security in cloud computing by implementing encrypted digital signatures with elliptic curve cryptography.

Goswani and Singh [24] developed an NP-complete class by solving equations over a ring of integers. The developed algorithm increases public encryption agreements and can be used in the server of a cloud computing service.

Van Dijk and Juels [25] noted that cryptography is not enough to increase cloud privacy, even though powerful tools, such as FHE. The results of this study were notable for its opposition to privacy leaking in cryptography.

Rocha and Correria [26] discussed the effects of a hypothetical malicious cloud on the confidential data of cloud users. This research topic is interesting because many clients that connect to clouds may upload several malware or viruses. Several clients even upload zombies for Botnet purposes. Thus, Rocha and Correria suggested the implementation of high privacy for each user through cryptographic operations.

Li et al. [27] used effective fuzzy keyword search for highly encrypted data in clouds to achieve high privacy. This concept based on fuzzy keyword search significantly enhanced system usability by matching files with the search inputs of users by searching inputs that exactly match the predefined keywords or, when an exact match is not found, the closest possible matching files based on keyword similarity semantics. The main principle behind the algorithm is that the measure to quantify keyword similarity is modified and an advanced technique for constructing the fuzzy keyword set system is developed to significantly reduce storage and representation overheads.

Agudo et al. [28] identified several cryptograph fields that can attract cloud computing providers. To produce a highly secure storage in cloud computing, the particular cryptographic solution must capture the attention of many

cloud providers and produce a high value monitoring level to reach satisfactory protection for consumer data.

Zhao et al. [29] studied the construction of a system for trusted data sharing through untrusted cloud providers to address the security issue. The constructed system can impose the access control policies of data owners and prevent cloud storage providers from unauthorized access and illegal authorization to access data.

Atyero and Feyisetan [30] studied the secure delivery of data sessions to and from the cloud and noted serious issues on such delivery. This study presented a new and effective security solution for issues that affect cloud computing. Atyero and Feyisetan proposed the use of homomorphic encryption to address serious security concerns in terms of access to cloud data.

Jaatun et al. [31] developed a confidentiality algorithm for cloud computing. An important finding of their research was the redundant array of independent net-storages (RAIN) for cloud computing. The RAIN approach divides data into segments and distributes them. Keeping the relation between the distributed segments private prevents the reassembly of the original data. Each segment is too small to disclose any meaningful information. RAIN ensures the confidentiality of data stored in the cloud.

VI. Discussion

Cloud computing has presented issues regarding data control, the effect of software systems on organic resources, and the transfer of data access control to another. Based on the above literature review, we conclude that cryptography can be used for the following:

- Proofs of irretrievability.
- Homomorphic encryption.
- Private information retrieval.
- Broadcast encryption.
- Knowledge and zero-knowledge proofs.
- Short signatures.

Thus, Fig. 5 Shown the ideas of cryptography usage through the three main security concept Confidentiality, Integrity and Availability (CIA).

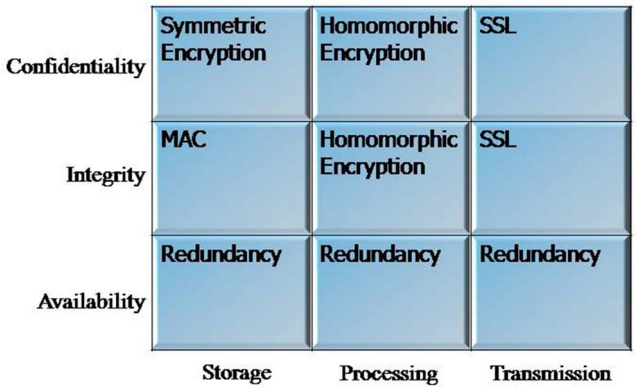

Fig.5. CIA over cloud

As a result, the benefits from cloud have spread widely through the backbone. But, the sandwich of cloud computing can't be complete without security Algorithms, encryption, and security policy. In addition when there are many securities implementation through multi-cloud there will be another obstacle which is performance. And how can manipulate thesis cryptography encryption things using large keys in less cost, but the clue not finishing yet. However, Availability is important after security and performance. Due to the fact in Fig.6, it conclude that security take the vast majority in comparing with other cloud factor that based on concept , and end point that represent by user, for example, sitting at home ,and upload data from client computer to the cloud point. There for, noting complete, and perfect in cloud computing security. But, many valuable researches, and real time produced high, and efficient solution for cloud computing world.

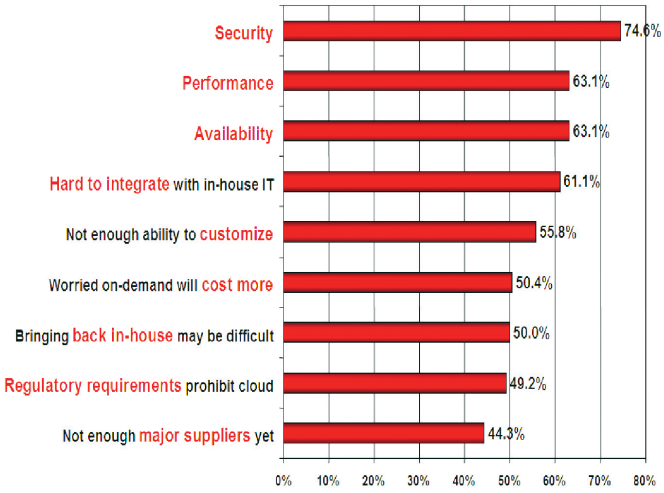

Fig. 6. Cloud usage vision

VII. Conclusion

Although there has been some increase in security cloud computing world, no straight solution under applied cryptographic implementation. A shared of ownership

between crypto algorithm and security policy might be collaborative approach for cloud computing. Therefore, our believe this improvement alone is not enough. From our surveyed paper, a conclusion led us to suggest, however third-party box work as gateway between client, and cloud which work as crypto box, or develop program work as encryption/decryption mechanism that maybe built-in between client's and cloud server as cryptography secure session's agreement.

ACKNOWLEDGMENT

The authors would like to thank the members in the Malaysia Greater Research Network System (MyGRANTs) Project especially Cloud & Security Research Group for their helpful discussions and suggestions. This work was supported by MyGRANTs Project, Ministry of Higher Education (MOSTI) Malaysia.

REFERENCES

[1] P. Mell, and T. Grance, "The NIST definition of cloud computing (draft)," *NIST special publication,* vol. 800, no. 145, pp. 7, 2011.

[2] S. Hillier, and T. Pattison, *Microsoft SharePoint 2013 app development*: Microsoft Press, 2012.

[3] J. Davis, *Teach Yourself VISUALLY Salesforce. com*: Wiley. com, 2013.

[4] R. Paul, "Checkpoint-based Intelligent Fault tolerance For Cloud Service Providers," *INTERNATIONAL JOURNAL OF COMPUTERS & DISTRIBUTED SYSTEMS,* vol. 2, no. 1, pp. 59-64, 2012.

[5] G. Ercolani, "Cloud Computing Services Potential Analysis. An integrated model for evaluating Software as a Service," *Cloud Computing*, pp. 77-80, 2013.

[6] A. Antonova, E. Gourova, and N. Roumen, "Extended architecture of knowledge management system with Web 2.0 technologies." pp. 48-55.

[7] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," *ACM SIGCOMM Computer Communication Review,* vol. 39, no. 1, pp. 50-55, 2008.

[8] Z. Yuan, G. Su, and W. Xiaoyun, "Contrast Study on Two Kinds of SIP Trunking Route Scheme Based IMS Network." pp. 1213-1218.

[9] A. Kütt, and K. Papamiltiadis, "Communication system and method," Google Patents, 2012.

[10] S. Bleikertz, S. Bugiel, H. Ideler, S. Nürnberger, and A.-R. Sadeghi, "Client-controlled Cryptography-as-a-Service in the Cloud."

[11] S. Sanyal, and P. P. Iyer, "Cloud Computing--An Approach with Modern Cryptography," *arXiv preprint arXiv:1303.1048*, 2013.

[12] W. Mao, "The role and effectiveness of cryptography in network virtualization: a position paper." pp. 179-182.

[13] K. Rauber, "CLOUD CRYPTOGRAPHY," *International Journal of Pure and Applied Mathematics,* vol. 85, no. 1, pp. 1-11, 2013.

[14] Y. Zheng, "Public Key Cryptography for Mobile Cloud," *Information Security and Privacy*, Lecture Notes in Computer Science C. Boyd and L. Simpson, eds., pp. 435-435: Springer Berlin Heidelberg, 2013.

[15] F. Kerschbaum, "Searching over encrypted data in cloud systems," in Proceedings of the 18th ACM symposium on Access control models and technologies, Amsterdam, The Netherlands, 2013, pp. 87-88.

[16] V. Ustimenko, and A. Wroblewska, "On some algebraic aspects of data security in cloud computing," *Proceedings of Applications of Computer Algebra ACA 2013. Málaga*, pp. 155, 2013.

[17] T. K. Chakraborty, A. Dhami, P. Bansal, and T. Singh, "Enhanced public auditability & secure data storage in cloud computing." pp. 101-105.

[18] A. Jangra, and R. Bala, "PASA: Privacy-Aware Security Algorithm for Cloud Computing," *Intelligent Informatics*, pp. 487-497: Springer, 2013.

[19] K. Wazed Nafi, T. Shekha Kar, S. Anisul Hoque, and M. Hashem, "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing Security Architecture," 2013.

[20] D. Eyers, and G. Russello, "Toward Unified and Flexible Security Policies Enforceable within the Cloud." pp. 181-186.

[21] Y. Dodis, W. Luo, S. Xu, and M. Yung, "Key-insulated symmetric key cryptography and mitigating attacks against cryptographic cloud software." pp. 57-58.

[22] M. Sudha, "Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography," *Advances in Computer Science and its Applications,* vol. 1, no. 1, pp. 32-37, 2012.

[23] V. Gampala, S. Inuganti, and S. Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography," *International Journal of Soft Computing and Engineering (IJSCE) ISSN*, pp. 2231-2307, 2012.

[24] B. Goswani, and D. S. Singh, "Enhancing Security in Cloud computing using Public Key Cryptography with Matrices," *International Journal of Engineering Research and Applications,* vol. 2, no. 4, pp. 339-344, 2012.

[25] M. Van Dijk, and A. Juels, "On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing," *IACR Cryptology ePrint Archive,* vol. 2010, pp. 305, 2010.

[26] F. Rocha, and M. Correia, "Lucy in the sky without diamonds: Stealing confidential data in the cloud." pp. 129-134.

[27] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing." pp. 1-5.

[28] I. Agudo, D. Nuñez, G. Giammatteo, P. Rizomiliotis, and C. Lambrinoudakis, "Cryptography goes to the Cloud," *Secure and Trust Computing, Data Management, and Applications*, pp. 190-197: Springer, 2011.

[29] G. Zhao, C. Rong, J. Li, F. Zhang, and Y. Tang, "Trusted data sharing over untrusted cloud storage providers." pp. 97-103.

[30] A. A. Atayero, and O. Feyisetan, "Security issues in cloud computing: The potentials of homomorphic encryption," *Journal of Emerging Trends in Computing and Information Sciences,* vol. 2, no. 10, pp. 546-552, 2011.

[31] M. G. Jaatun, A. A. Nyre, S. Alapnes, and G. Zhao, "A farewell to trust: An approach to confidentiality control in the Cloud." pp. 1-5.

View publication stats