ZIBELINE INTERNATIONAL™ PUBLISHING

Matrix Science Mathematic (MSMK)

DOI: http://doi.org/10.26480/msmk.02.2022.52.57

ISSN: 2521-0831 (Print)
ISSN: 2521-084X(Online)
CODEN: MSMAD

RESEARCH ARTICLE

CLOUD COMPUTING'S USE OF CRYPTOGRAPHY

Rajesh De, Ipseeta Nanda, Varsha kumari

Faculty of Information Technology, Gopal Narayan Singh University, Jamuhar, Sasaram, Bihar-821305, India.
****Corresponding Author email: ipseeta.nanda@gmail.com***

ARTICLE DETAILS

Article History:

Received 09 September 2022
Revised 13 October 2022
Accepted 17 November 2022
Available online 23 November 2022

ABSTRACT

Cloud computing is a platform for dynamically enhancing capabilities and increasing potentialities without requiring the addition of new hardware, employees, or software. Additionally, cloud computing began as a business notion and later became a successful IT innovation. Concerns have been expressed about the security of the cloud environment, though, considering that the cloud contains a lot of information about people and businesses. Although cloud computing has received a lot of attention, clients are still hesitant to move their businesses there. However, the only significant issue preventing greater adoption of cloud computing is a lack of protection. Additionally, the market is wary about cloud computing due to the intricacy with which it controls data protection and confidentiality. When used in a cloud context, the cloud model architecture jeopardises the security of current technology. Therefore, cloud service customers should be aware of the risks associated with uploading data into this novel environment. Therefore, several areas of cryptography that endanger cloud computing are examined in this work. This paper provides an overview of the specific security concerns that using cryptography in a cloud computing system raises.

KEYWORDS

Cloud security infrastructure, cryptographic techniques, and cloud encryption

1. INTRODUCTION

Depending on it, and the words and ideas connected to it offer considerable understanding. The definition of cloud computing as it exists has been muddled by literature. However, many businesses cater to their service requirements at the place where the phrase "cloud computing" first appeared—the network topology. In Figure a typical cloud is displayed. The practise of using actual applications or services over the Internet is referred to as cloud computing (Mell and Grance, 2011). Cloud computing did not evolve quickly; it may be somewhat traced back to a time when computing systems had remotely time-shared computing resources and useful applications. Concerns have been expressed about the various types of applications and the services that they access through clouds. Many times, the equipment and software used to provide these services don't have any unique capabilities. Many businesses use cloud-based services. The following is an example of a company that utilised cloud computing services in 2010: Microsoft offers the Microsoft® SharePoint® online service, which Office useful software are made available in the cloud, together with content and corporate enterprise intelligence technologies. For official users and major infrastructure IT firms, Google Cloud Storage offers a wide range of services (Hillier and Pattison, 2012).

Salesforce.com also created its own cloud services for its clients (Davis, 2013). Additionally, Vmforce and other commercial providers have developed into mature cloud services in recent years (Paul, 2012). However, it's possible that the cloud clue is still unclear, leaving the question of just what and why cloud computing exists. Whose concern is the cloud platform, and what about encryption and security? The parts that follow attempt to provide a clear understanding of service model z, traits, deployment models, benefits, and cryptography features with cloud computing.

2. ASPECTS OF CLOUD COMPUTING

The following are the most significant features of cloud computing:

2.1 Distributed Infrastructure

A virtualized software architecture, for instance, networking capabilities, and optionally shared physical services are all features of cloud computing. Further, storage can also be done using cloud computing. Regardless of the deployment option, the cloud infrastructure constructs visible infrastructure in accordance with the estimated user count.

2.2 Dynamic Provisioning

Through software automation, services are automatically permitted for actual necessity. It is optional to elaborate and compress service capacity. These dynamic scaling requirements are targeted while upholding a high level of safety and reliability.

2.3 Network Access

To achieve universal access to devices, such as PCs, laptops, and mobile devices, using standard-based API representations developed on HTTP, a network connection is necessary. Applications for everyday corporate use as well as cutting-edge applications for the newest smartphones are deployed via cloud services.

2.4 Managed Metering

In cloud computing, a metre is used to manage and optimise service as well as to provide reporting and billing data. Almost anywhere can access multiple shared and scalable services thanks to cloud computing. Based on actual consumption, the consumer gets charged for these services.

Quick Response Code	Access this article online	
	Website: www.matrixsmathematic.com	**DOI:** 10.26480/msmk.02.2022.52.57

Cite The Article: Rajesh De, Ipseeta Nanda, Varsha kumari (2022). Cloud Computing's Use of Cryptography. *Matrix Science Mathematic, 6(2): 52-57.*

3. Product Models

When cloud computing originally emerged, its services were implemented in environments with high demands in the corporate world, as seen in Figure 2. Examples of typical services include:

3.1 Software as a Service (SaaS)

Customers purchase the right to utilize a cloud-based application or service (Ercolani, 2013). Microsoft is becoming more active in this field. Microsoft's Office Web Apps are available to Office volume license clients and Office Web App subscribers through its cloud-based web services as part of the cloud computing option for Microsoft Office 2010.

3.2 Platform as a Service (PaaS)

Users pay a monthly subscription fee to access platforms so they can upload their own programmes and programmes into the cloud (Antonova et al., 2009). Operating systems and network access are not controlled by consumers, and there may be limitations on the kind of apps that can be built.

3.3 Infrastructure as a Service (IaaS)

Users don't just maintain the cloud infrastructure; they also control and manage system operations, applications, storage, and network connectivity. Additionally, distinct subgroups of these cloud models in a market or industry are identified. One such subset model used to distinguish hosted IP telephony services is communications as a service (CaaS) (Vaquero et al., 2008). CaaS prompted a change toward more IP-centric communication and a large-scale deployment of SIP trunks (Yuan et al., 2012). Private branch exchange (PBX) entry into the cloud is facilitated by the installation of IP and SIP (Kutt and Papamiltiadis, 2012). CaaS can be viewed as a subset of SaaS deployment models in this situation.

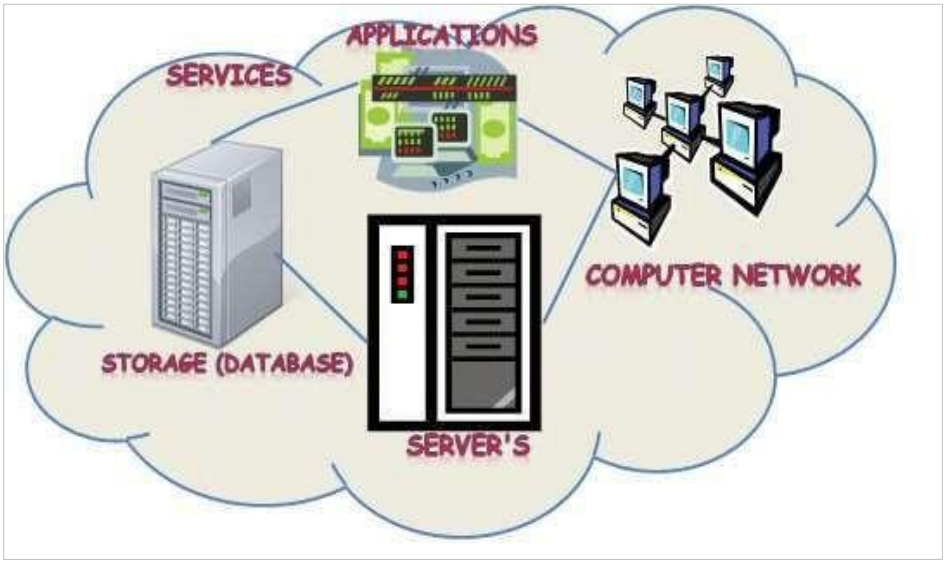

Figure 1: Utilizing the cloud

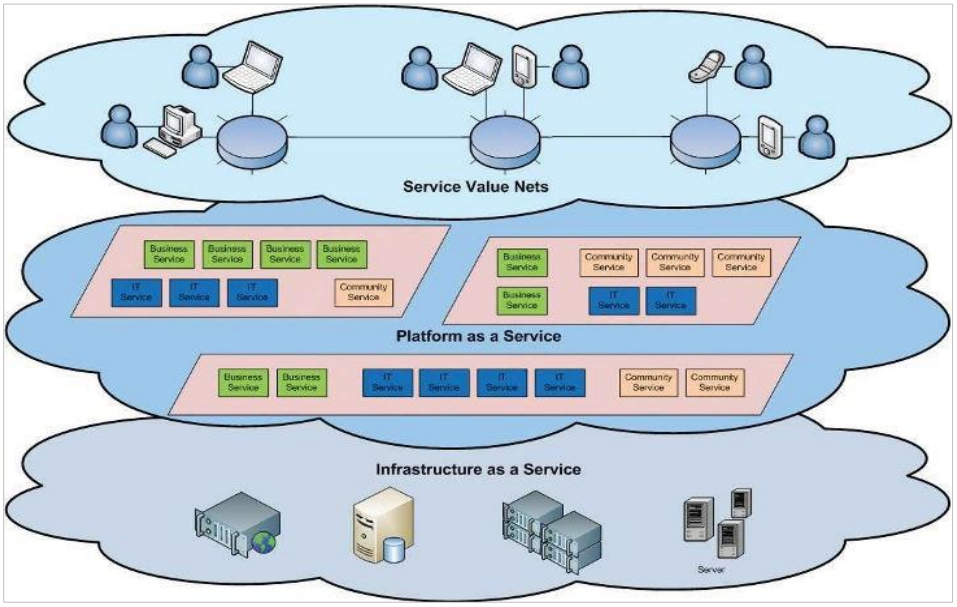

Figure 2: Model of service

3.3.1 Models for Cloud Deployment

The four deployment models that can be used to address the requirements concerns in Define Cloud computing are as follows:

Private Cloud: is set up, monitored, and used for a certain geographic area. However, due to an internet connection, it will be abroad. however, from a private branch.

Public cloud: Users of the public can access public cloud infrastructure, such as the Google Drive service. On contrast to the capital typically required with other cloud computing services, the public cloud actually enables a consumer to design and launch a service in the cloud with very little financial outlay.

Hybrid Cloud: Any cloud infrastructure has a number of clouds spread across several locations. Information, or incomplete information that permitted moving between clouds, is only possible in the clouds. On order to satisfy the needs of maintaining corporate data and providing services in the cloud, private and public clouds can be combined.

Community Cloud: This cloud is used for significant infrastructure, such as

connecting government agencies to one cloud to upload data with unified information or a campus server that connects a single cloud computing community.

While in Figure 3, It also demonstrates that 35% of IT users do not use cloud servers due to security concerns. These consumers need to be aware of other unsecure cloud computing services. As a result of the high cost of servers due to their dependence on hardware, software, and the skills needed to implement them, the number of users of private clouds has quietly increased these elements. 17% of all cloud servers are made up of public cloud servers. Free primary cloud providers like MSN, Yahoo, and Google offer public cloud servers as part of their free offerings. Because the expenses for combining private and public clouds are reasonable, hybrid clouds may be the most developed service in the world.

As was already said, cloud computing assaults are receiving more and more attention. These assaults may be carried out for a variety of reasons, such as to obtain important information about significant businesses or to forge personal data. Figure 4 is an illustration of how an attacker might get past a virtual machine and enter the cloud environment's hypervisor.

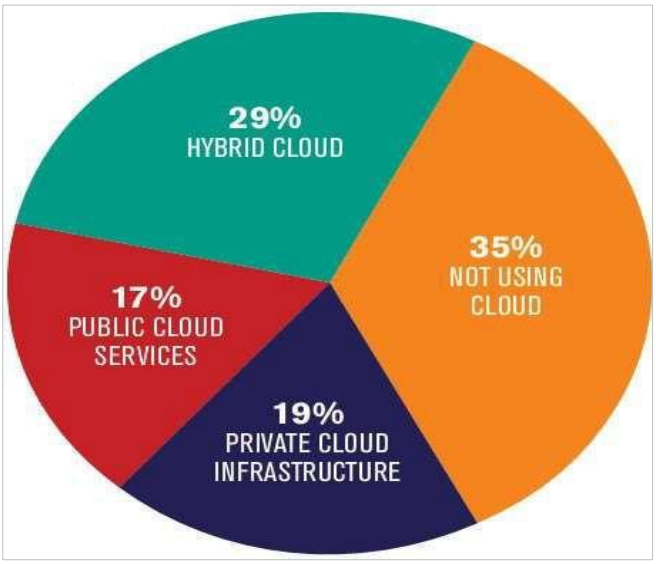

Figure 3: Use of cloud computing

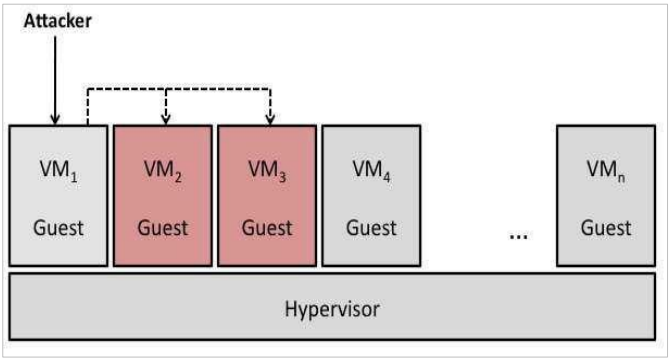

Figure 4: An illustration of a virtual machine attack

4. Cross-Security and Cloud Computing

Clear text is changed by cryptography into an unintelligible format. By assuring that only the intended recipient can see the information, the technology of cryptography is routinely used to transport data securely. This domain focus offers a summary of the development of cryptography and the numerous Modern enterprise encryption uses sophisticated, creative methods.

4.1 Internet of Things Encryption

The importance of encryption in the area of cloud computing must be investigated in numerous studies. Identification based on encryption is one of the main areas of focus for encryption in cloud computing. Here is an illustration of encryption:

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.

4.2 Review of Research on Cryptography for Cloud Computing

The secret key concepts were put forth and applied to virtual machines on the foundation of a special client- controlled CaaS architecture for cloud computing (Bleikertz et al., 2013). The management and storage of cloud customers' keys as well as all cryptographic operations are segregated inside a secure crypto domain called DomC, which is tightly tied to the workloads of clients, according to these researchers, who focused on the usage of physical hardware security modules. While Sanyal and Iyer looked on public key values' effects on cloud security (Salyal and Iyer, 2013). They talked about a reliable, effective approach based on the 128/192/256-bit cypher key utilised in the multi-key AES encryption method. Results showed that using AES rather than RSA improved cloud computing security. AES, however, is compatible with virtual machines and both public and private clouds.

An key issue for secure network virtualization was brought up by Mao: hypervisors' careless use of distributed power and intelligence (Mao, 2013). The study covered how hypervisors take command by using information boxes. As a result, he suggested network virtualization, which has a number of practical uses, such as safe multi-tenancy for cloud computing. The management of the intelligence and distributed power of hypervisors is heavily impacted by cryptography. In order for the system

to function, cloud computing security is a need, according (Rauber, 2013). In fact, Rauber questioned whether cloud computing will fundamentally alter computing experience and emphasised that its core components should be secure. The study also looked at how SaaS, homomorphic encryption, and functional encryption function and how they protect data. These subjects were thoroughly explored, and insightful conclusions were reached.

Zheng created a mobile cloud with increased security in order to address the particular problem provided by security (Zheng, 2013). Through the use of public key cryptography, Zaheng created encrypted data so that a sender may get information from a cypher text saved in the cloud without depending on the recipient. An important concern in cloud computing is privacy. While on Facebook, content can be shared using the Share button on platforms like Twitter and LinkedIn. However, Zaheng noted that there is still a serious security risk when using mobile cloud computing servers to access social media. Infrequent queries, security versus performance query optimization, and access control are just a few of the major cloud security challenges that Kerchbaun found (Kerschbaum, 2013). He then created a high-performance prototype that may be used in real-world applications.

Ustimenko and Wroblewska discovered that algebra is crucial for cryptography for the security of cloud computing and offered a wonderful idea for homomorphic encryption and multivariate key cryptography (Ustimenko and Wroblewska, 2013). Ellipstic curve cryptography was suggested for a homomorphic encryption system (Chakraborty et al., 2013). A high data self-control method resulted from the initial implementation. The programme validated the retrievability scheme, allowing the client to contest the accuracy of the data that was being saved. Since concept is crucial for proposals in cryptography, Chakraborty et al. have relied on the idea that using a third-party auditor is a very secure technique. On behalf of the client, the idea was utilized to validate and alter secure path data. Because the creators believed that a Merkle hash tree securely expedites data access, it was employed for data server storage.

While various studies have criticized elliptic curve cryptography's high cost in PKI, this problem can only be solved by improving the ECC algorithm (Jangra and Bala, 2013). In order to create a privacy-aware security algorithm in the cloud, Jangar and Bala used RSA. They discovered that the algorithm is effective, secure, and private when used in the cloud. Important studies on cloud security have looked at secure cryptographic pathways, including data integrity and privacy (Nafi et al., 2013). The withholding of information from clients and users has not been the subject of many studies. Therefore, some reseaerchers presented an enhanced AES encryption method for concealing information sessions between clients and servers as a secure technique to build cloud computing platforms (Nafi et al., 2013). This concept includes asynchronous key systems for communication or data exchange and AES- based file encryption systems. AsIn order to protect information from traces and packets delivered to the cloud infrastructure, PaaS, SaaS, and IaaS can employ AES for these three cloud models.

According to Eyers and Russello, as more people adopt the cloud computing trend, it will become more difficult (Eyers and Russello, 2013). Self-hosted resources pose a number of concerns to the cloud computing business model. Despite their unanticipated curiosity, customers do trust cloud computing and are interested in it. F, it offers big prime keys so that secure sessions can be created. However, many cloud applications' performance will be hampered by this technique. Key-insulated symmetric key cryptography, which lessens the harm caused by looping attacks against integrated cryptographic software, was examined (Dodis et al., 2012). They created a proof-of-concept kernel-based virtual machine environment and stressed the viability of symmetric key cryptography in key-insulated encryption.

As part of a security model for data security in cloud computing, Sudha investigated cloud security for data integrity, confidentiality, and authentication using a model that uses hyper crypto encryption for asymmetric and symmetric cryptographic algorithms (Sudha, 2012). A group researchers investigation on data security in cloud computing used elliptic curve cryptography to implement encrypted digital signatures (Gampala et al., 2012). In order to create an NP-complete class, Goswani and Singh had to solve equations over an integer ring (Goswani and Singh, 2012). The created technique strengthens existing public encryption agreements and can be applied to a cloud computing service's server.

Van Dijk and Juels pointed out that despite the efficacy of techniques like FHE, cryptography is insufficient to increase cloud privacy (Dijk and Juels, 2010). The study's findings stood in contradiction to privacy leakage in encryption. The repercussions of a hypothetical hostile cloud on the private information of cloud users were examined by (Rocha and Correria, 2011). Due to the possibility of several clients connecting to clouds uploading malware or viruses, this research issue is intriguing. Even more clients upload zombies for use by botnets. Rocha and Correria recommended that high privacy be implemented for each user through cryptographic processes.

To achieve great privacy, a group researchers used efficient fuzzy keyword search for securely encrypted data in clouds (Li et al., 2010). By matching files with search inputs that perfectly match the predefined keywords or, when an exact match is not found, the closest feasible matching files based on keyword similarity semantics, this approach based on fuzzy keyword search dramatically improved system usability. The algorithm's core idea is to greatly minimize storage and representation overheads by modifying the metric used to assess keyword similarity and developing a sophisticated method for building the fuzzy keyword set system. Several cryptograph areas have been highlighted as being attractive to cloud computing companies (Agudo et al., 2011). The specific cryptographic solution needs to gain the interest of many people in order to build a highly secure storage in cloud computing. To provide adequate protection for customer data, cloud providers and producers of high value monitoring levels.

To address the security issue, a group researchers researched the development of a system for trusted data sharing through dubious cloud providers (Zhao et al., 2010). The created system is capable of enforcing the access control regulations set forth by the owners of the data as well as shielding cloud storage providers from unlawful access and improper authorization to access data. In their study of the secure transfer of data sessions to and from the cloud, Atyero and Feyisetan identified significant problems with this transfer (Atayero and Feyisetan, 2011). This study offered a fresh and practical security fix for problems affecting cloud computing. Homomorphic encryption was the solution put up by Atyero and Feyisetan to overcome major security issues with regard to access to cloud data.

A confidentiality algorithm for cloud computing was created by Jaatun et al. The redundant array of independent net-storages (RAIN) for cloud computing was one of their study's key discoveries. Data is distributed and segmented using the RAIN method. The reassembly of the original data is prevented by keeping the relationship between the scattered parts a secret. The size of each piece makes it impossible to reveal any valuable information. RAIN guarantees the privacy of data kept in the cloud.

5. Discussion

Issues with data control, the impact of software systems on natural resources, and the transfer of data access control to another have been raised by cloud computing. The literature research mentioned above led us to the following conclusion about the applications of cryptography:

- Irretrievability evidence. Homomorphic cryptography
- The search for private information.
- Encryption for broadcasts.
- Proofs of knowledge and ignorance.
- Brief signatures such that Figure 5 Illustrated the principles of cryptography's application using the three key
- security concepts of confidentiality, integrity, and availability (CIA).

As a result, the advantages of the cloud have permeated the entire backbone. However, security algorithms, encryption, and security policy are necessary for the cloud computing sandwich to be complete. Additionally, performance will be a barrier when numerous security implementations occur through multi- cloud. And how can things be made more easily manipulable with huge keys at a lower cost, but the answer is still not complete. After security and performance, availability is crucial (Jaatun et al., 2011). Because of Figure 6, it is concluded that security dominates other cloud factors as compared to those based on concept and end points that represent users, such as those who are at home from the client computer, then upload data to the cloud location. Thus, it is important to note that cloud computing security is perfect and comprehensive. But numerous worthwhile studies and real-time innovations have generated effective and high-quality cloud computing solutions.

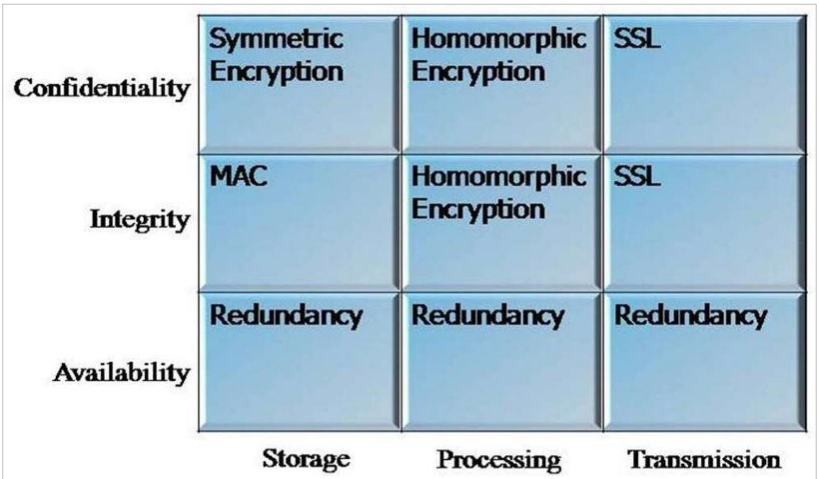

Figure 5: CIA regarding the cloud

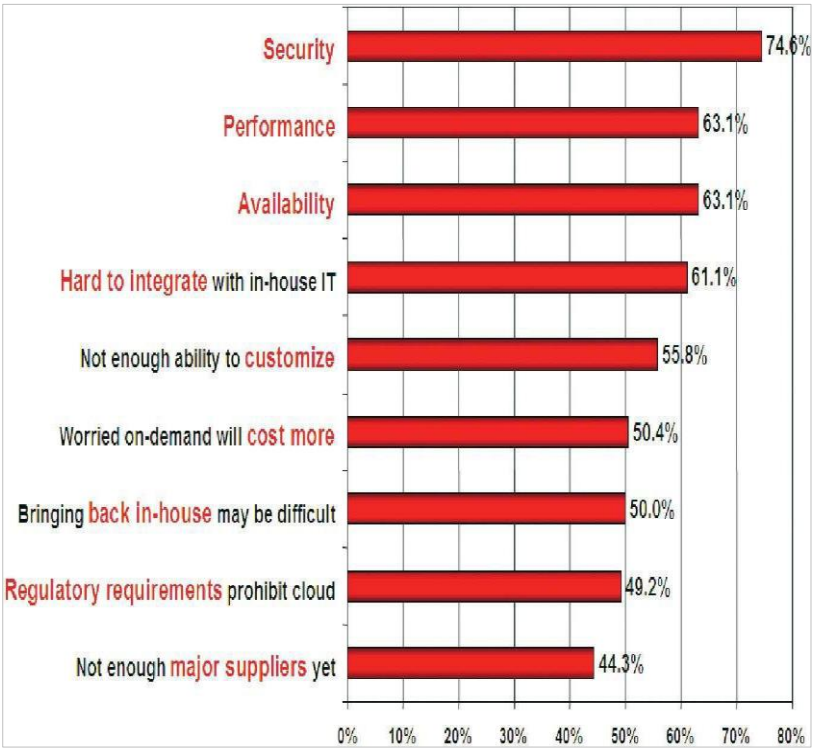

Figure 6: Vision for cloud usage

6. Conclusion

Despite a slight rise in cloud computing security, there is still no clear-cut cryptographic implementation solution. a proportionate ownership A cooperative strategy for cloud computing could be found between cryptographic algorithms and security regulations. We therefore think that this improvement alone is insufficient. As a result of our survey, we have come to the conclusion that either third-party boxes that act as a gateway between clients and the cloud and that function as crypto boxes, or programmes that work as encryption/decryption mechanisms that may be integrated between clients and cloud servers as part of a cryptography secure session's agreement, should be suggested.

References

Agudo, I., Nuñez, D., Giammatteo, G., Rizomiliotis, P., and Lambrinoudakis, C., 2011. Cryptography goes to the Cloud. Secure and Trust Computing, Data Management, and Applications, Pp. 190-197.

Antonova, A., Gourova, E., and Roumen, N., 2009. Extended architecture of knowledge management system with Web 2.0 technologies. Computer Science, Business, Pp. 48-55.

Atayero, A.A., and Feyisetan, O., 2011. Security issues in cloud computing: The potential of homomorphic encryption. Journal of Emerging Trends in Computing and Information Sciences, 2 (10), Pp. 546-552.

Bleikertz, S., Bugiel, S., Ideler, H., Nürnberger, S., Sadeghi, AR., 2013. Client-Controlled Cryptography-as-a-Service in the Cloud. In: Jacobson, M., Locasto, M., Mohassel, P., Safavi-Naini, R. (eds) Applied Cryptography and Network Security. ACNS 2013. Lecture Notes in Computer Science, vol 7954. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-38980-1_2

Chakraborty, T.K., Dhami, A., Bansal, P., and Singh, T., 2013. Enhanced public auditability & secure data storage in cloud computing, Pp. 101-105.

Davis, J., 2013. Teach Yourself VISUALLY Salesforce. com: Wiley. com.

Dijk, M.V., and Juels, A., 2010. On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing. IACR Cryptology ePrint Archive, Pp. 305.

Dodis, Y., Luo, W., Xu, S., and Yung, M., 2012. Key-insulated symmetric key cryptography and mitigating attacks against cryptographic cloud software. Pp. 57-58.

Ercolani, G., 2013. Cloud Computing Services Potential Analysis. An integrated model for evaluating Software as a Service. Cloud Computing, Pp. 77-80.

Eyers, D., and Russello, G., 2013. Toward Unified and Flexible Security Policies Enforceable within the Cloud. IFIP International Conference

on Distributed Applications and Interoperable Systems, Pp. 181-186.

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

Goswani, B., and Singh, D.S., 2012. Enhancing Security in Cloud computing using Public Key Cryptography with Matrices. International Journal of Engineering Research and Applications, 2 (4), Pp. 339-344.

Hillier, S., and Pattison, T., 2012. Microsoft SharePoint 2013 app development: Microsoft Press.

Jaatun, M.G., Nyre, A.A., Alapnes, S., and Zhao, G., 2011. A farewell to trust: An approach to confidentiality control in the Cloud. 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology (Wireless VITAE), Pp. 1- 5.

Jangra, A., and Bala, R., 2013. PASA: Privacy-Aware Security Algorithm for Cloud Computing. Intelligent Informatics, Pp. 487- 497.

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

Kütt, A., and Papamiltiadis, K., 2012. Communication system and method. Google Patents.

Li, J., Wang, Q., Wang, C., Cao, N., Ren, K., and Lou, W., 2010. Fuzzy keyword search over encrypted data in cloud computing. Proceedings IEEE INFOCOM, Pp. 1-5.

Mao, W., 2013. The role and effectiveness of cryptography in network virtualization: a position paper. ASIA CCS '13: Proceedings of the 8th ACM SIGSAC symposium on Information, computer, and communications security, Pp. 179-182.

Mell, P., and Grance, T., 2011. The NIST definition of cloud computing (draft). NIST special publication, 800 (145), Pp. 7.

Nafi, K.W., Kar, T.S., Hoque, S.A., and Hashem, M., 2013. A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing Security Architecture.

Paul, R., 2012. Checkpoint-based Intelligent Fault tolerance For Cloud Service Providers. International Journal of Computers & Distributed Systems, 2 (1), Pp. 59-64.

Rauber, K., 2013. Cloud Cryptography. International Journal of Pure and Applied Mathematics, 85 (1), Pp. 1-11.

Rocha, F., and Correia, M., 2011. Lucy in the sky without diamonds: Stealing confidential data in the cloud. IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W), Pp. 129- 134.

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

Sudha, M., 2012. Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography. Advances in Computer Science and its Applications, 1 (1), Pp. 32-37.

Ustimenko, V., and Wroblewska, A., 2013. On some algebraic aspects of data security in cloud computing. Proceedings of Applications of Computer Algebra ACA, Málaga, Pp. 155.

Vaquero, L.M., Rodero-Merino, L., Caceres, J., and Lindner, M., 2008. A break in the clouds: towards a cloud definition. ACM SIGCOMM Computer Communication Review, 39 (1), Pp. 50-55.

Yuan, Z., Su, G., and Xiaoyun, W., 2012. Contrast Study on Two Kinds of SIP Trunking Route Scheme Based IMS Network. Proceedings of the 2012 International Conference on Communication, Electronics and Automation Engineering, Pp. 1213–1218 .

Zhao, G., Rong, C., Li, J., Zhang, F., and Tang, Y., 2010. Trusted data sharing over untrusted cloud storage providers. Proceedings of the 2010 IEEE Second International Conference on Cloud Computing Technology and Science, Pp. 97-103.

Zheng, Y., 2013. 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.