IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11653

USAGE OF CRYPTOGRAPHIC IN CLOUD COMPUTING

Er.Rohini

Assistant Professor, CGC, Jhanjeri, Punjab

Abstract: Cloud computing is a platform for dynamically growing capabilities and increasing potentialities without the need for new infrastructure, staff, or software. Furthermore, cloud computing began as a commercial enterprise notion and has since grown into a thriving IT technology. However, considering that the cloud stores a great deal of information about individuals and businesses, worries about the cloud's security have been raised. Despite all of the buzz around cloud computing, clients are still hesitant to move their businesses to the cloud. Nonetheless, the lack of security is the single major problem that is preventing more people from using cloud computing. Furthermore, the market is wary about cloud computing due to the intricacy with which it controls data confidentiality and information security.When established technologies are employed in a cloud environment, the architecture of cloud models poses a security risk. As a result, users of cloud services should be aware of the risks associated with uploading data into this new environment. As a result, numerous cryptographic features that represent a threat to cloud computing are examined in this research. This study examines the security concerns raised by the usage of cryptography in a cloud computing environment.

Index Terms: Cloud encryption, cryptographic algorithms,cloud security infrastructure.

I. INTRODUCTION

You can rely on it, and the terminology and concepts associated with it may offer you with a wealth of information. Cloud computing literature has muddied the fundamental concept of cloud computing. Many firms, on the other hand, base their service needs on network topology, which is where the term "cloud computing" comes from. A classic cloud is depicted in Figure 1. The use of the Internet to execute actual programmes or services is known as cloud computing [1]. Cloud computing did not emerge out of nowhere; it can be traced back to a time when computers had remote time-shared computing resources and practical applications. Concerns have been expressed about the many types of apps and services fetched via clouds. In many cases, the devices and apps employed in these services perform no unusual tasks. Many businesses use cloud-based services. In 2010, a company that used cloud computing services produced the following results: Microsoft offers the Microsoft® SharePoint® online service, which allows users to upload material and business intelligence tools to the cloud and access office applications from anywhere.

Many services are provided by Google cloud storage for formal customers and major infrastructure I.T organisations [2]. Salesforce.com also developed its own cloud services for its customers [3]. Furthermore, Vmforce and other premium cloud services have grown up in recent years [4]. However, the cloud clue may not be evident yet, and a query may be posed as to what cloud computing is and why it is used. Who is responsible for the cloud platform, and what about security and encryption? The following sections attempt to provide a comprehensive understanding of cloud computing service models z, characteristics, deployment models, benefits, and cryptography features.

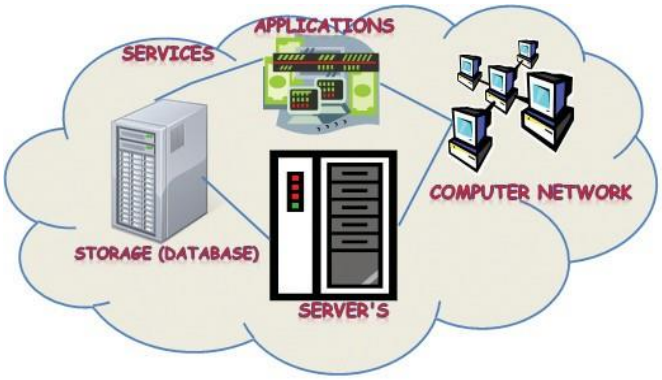


Fig. 1. Cloud computing

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11653

II.CLOUD COMPUTING FEATURES

Cloud computing consumes various features, the most vital of which are as follows:

1. Distributed Infrastructure: Cloud computing has a virtualized software framework, for example, networking capabilities, and optionally sharedphysical 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: Software automation allows for the automatic provisioning of services based on actual need. It is optional to elaborate and compress service capacity. These dynamic scaling requirements are met while maintaining high levels of dependability and security.

3. Network Access: By using standard-based API representations developed on HTTP, an Internet connection is necessary to achieve across-the-board access to devices such as PCs, laptops, and mobile devices. Cloud-based deployments range from realistic corporate applications to cutting-edge apps for the latest smart phones.

4. Managed Metering: In cloud computing, a meter is used to manage and optimise service, as well as to provide reporting and billing data. Cloud computing allows users to access a variety of shared and scalable services from virtually anywhere. These services are billed based on actual usage.

II. PROVISION MOCKUPS

When cloud computing was first shaped, the facilities it obtainable were organized in business circumstances with high strains as shown in Fig.2. Common provision illustrations contain:

- Software as a Service (SaaS): Consumers purchase the opportunity to access and use a cloud-based application or service [5]. Microsoft is stepping up its efforts in this area. Microsoft's Office Web Apps are available through its cloud-based internet services to Office volume licence clients and Office Web App customers as part of the cloud computing alternative for Microsoft Office 2010.
- Platform as a Service (PaaS): Consumers buy access to platforms that allow them to upload their own software and apps to the cloud [6]. Consumers may not have control over operating systems or network access, and there may be limitations on which programmes can be installed.
- Infrastructure as a Service (IaaS): Consumers not only maintain the cloud infrastructure, but also control and manage system operations, applications, storage, and network connectivity [7]. Furthermore, the many subgroups of these cloud models in a particular business or market are identified. One such subset model used to distinguish hosted IP telephony services is Communications as a Service (CaaS). CaaS prompted a transition to more IP-centric communications and the implementation of multiple Session Initiation Protocol (SIP) trunks [8]. The cloud entrance of a private branch exchange (PBX) is facilitated by installing IP and SIP [9]. CaaS might be considered as a subset of SaaS deployment models in this scenario.
-

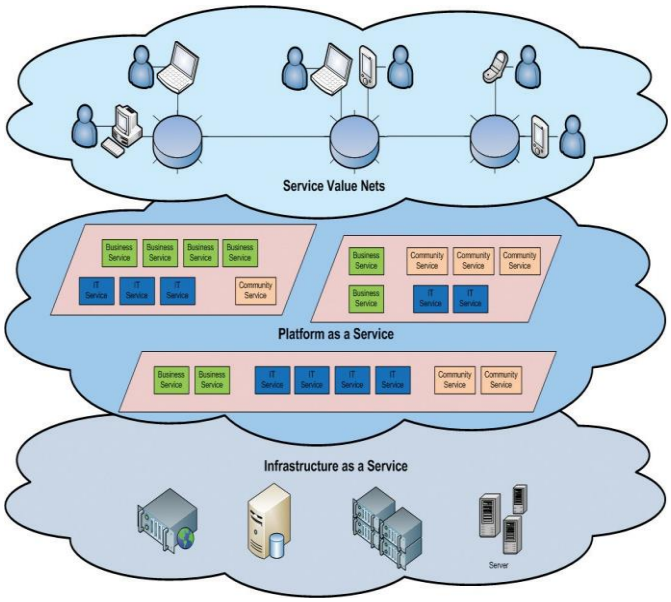


Fig.2. Service model

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11653

A. Cloud deployment models

The four deployment models that can be used to solve these difficulties are as follows: Define Cloud computing has requirements concerns; the four deployment models that can be used to address these issues are as follows::

1. Private Cloud: It is deployed, monitored, and engaged for a specific range of distance. However, it will be done on the internet from afar. However, from a private branch-branch perspective.
2. Public Cloud: Infrastructure, such as Google Drive, is available to the whole public. On reality, as compared to the capital required with other cloud computing services, public cloud allows a consumer to design and launch a service in the cloud with relatively minimal outlay.
3. Hybrid Cloud: Any cloud infrastructure would have multiple clouds in various locations. Only information, or partial information that enabled movement between clouds, is allowed by the clouds. To satisfy the requirements of maintaining corporate data and offering cloud services, private and public clouds can be combined.
4. Community Cloud: This cloud is used for huge infrastructure, such as government entities connecting to a single cloud to upload data with uniform information or a campus server connecting a single cloud computing community.

While, in Fig.3. Also shows that Because of security concerns, 35% of information technology users do not use cloud servers. Other cloud computing services lacking security must be made known to these users. Because the cost of servers is based on hardware, software, and the skills necessary to implement them, the number of private cloud users has gradually increased.

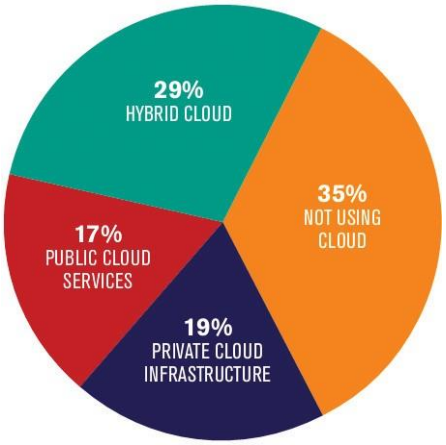
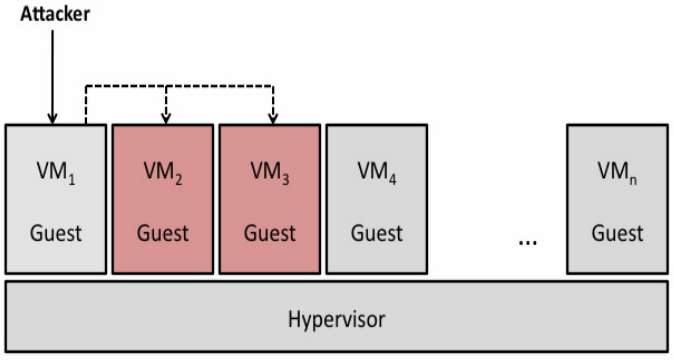


Fig.3. Cloud computing usage

these components. The entire number of cloud servers is made up of 17% public cloud servers. Free primary cloud providers such as MSN, Yahoo, and Google provide public cloud servers. Because the prices of combining private and public clouds are reasonable, hybrid clouds may be the most developed service on the planet.

As previously said, cloud computing hacks are receiving more attention. These attacks could be carried out for a variety of reasons, including acquiring important information on large-scale businesses or fabricating personal data. Figure 4 illustrates how anattacker can gain access to a virtual machine's hypervisor in a cloud environment.



.

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

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11653

III. CLOUD COMPUTING AND CRYPTOGRAPHIC

Cryptography is the process of converting plain text into an unreadable format. Cryptography is a common method for securely transferring data by assuring that only the intended receiver may read it. This domain spotlight gives an overview of cryptography's history as well as the numerous complicated and innovative ways employed in modern enterprise encryption.

A. Cloud computing encryption

Encryption in the cloud computing industry is a critical problem that requires further research. One of the main objectives of encryption in cloud computing is encryption-based identification. The following is an example 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.

ANALYSIS OF STUDIES ON CRYPTOGRAPHY FOR CLOUDCOMPUTING

On the basis of a unique client-controlled CaaS architecture for cloud computing, Bleikertz et al. [10] introduced the secret key principles, which are applied to virtual machines. These researchers, on the other hand, emphasised the use of physical hardware security modules, and discovered that the architecture separates the management and storage of cloud clients' keys, as well as all cryptographic operations, into a secure crypto-domain called DomC, which is tightly coupled to client workloads..

Sanyal and Iyer [11], on the other hand, looked at cloud security using public key values. They talked about a safe and efficient approach based on the AES technique, which uses a 128/192/256 bit cypher key to encrypt and decrypt data. When compared to RSA, the results show that AES improves cloud computing security. AES, on the other hand, can be employed in virtual computers as well as public and private clouds.

Mao [12] identified a major issue for secure network virtualization: hypervisors' sloppy use of intelligence and distributed power. The study looked at how hypervisors take control by using information boxes. As a result, he proposed network virtualization, which he said could be used for a variety of purposes, including secure multi-tenancy for cloud computing. Cryptography has a big impact on how hypervisors manage their intelligence and distributed power.

Rauber [13] investigated cloud computing security, which is required by the entire system or it will collapse. In fact, Rauber contended that the main components of a cloud should be safe, and he debated whether cloud computing will revolutionise computing. The study also looked at the functionalities of SaaS, homomorphic encryption, and functional encryption, as well as their security techniques. These topics were thoroughly discussed, with useful outcome.

By creating an upgraded security-mobile cloud, Zaheng [14] focused on the unique problem given by security. Zaheng defined public key cryptography as a way for a sender to access data from a cypher text stored in the cloud without relying on the cypher text's recipient. In cloud computing, privacy is a major concern.

While material on Facebook can be shared on other social networks like Twitter and LinkedIn via the Share button. Zaheng, on the other hand, believes that using mobile cloud computing servers while accessing social media sites is still a serious security risk.

Kerchbaun [15] recognised many key cloud security challenges, including infrequent queries, security versus performance query optimization, and access control, and created a high-performance prototype suited for widespread implementation.

Ustimenko and Wroblewska [16] proposed a wonderful idea for homomorphic encryption and multivariate key cryptography, and discovered that algebra is crucial for cloud computing security cryptography.

Kerchbaun [15] recognised many key cloud security challenges, including infrequent queries, security versus performance

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022
DOI: 10.17148/IJARCCE.2022.11653

query optimization, and access control, and created a high-performance prototype suited for widespread implementation. Ustimenko and Wroblewska [16] proposed a wonderful idea for homomorphic encryption and multivariate key cryptography, and discovered that algebra is crucial for cloud computing security cryptography.
Several studies in PKI have complained about the high cost of elliptic curve cryptography; this excessive cost can only be reduced by improving the ECC algorithm [18]. Jangar and Bala employed RSA to build a privacy-aware security algorithm in the cloud, and discovered that the algorithm is efficient, secure, and private when used in the cloud.

Secure paths for cryptography, such as privacy and data integrity, have been studied in important studies on cloud security [19]. The concealing of information from clients and users has been the subject of few research. Wazed Nafi et al. suggested an enhanced AES encryption scheme for hiding information sessions between clients and servers as a secure technique to build cloud-computing systems. This architecture includes AES-based file encryption systems and asynchronous key systems for sharing information or data. As a result, PaaS, SaaS, and IaaS can employ AES to mask information from traces and packets transferred to the cloud infrastructure in these three cloud models.
The cloud computing trend, according to Eyers and Russello [20], will become increasingly complex as the number of consumers grows. Self-hosted resources pose a number of concerns to cloud computing's concept. In fact, consumers trust cloud computing, and they are fascinated about it, even if it is unintentional. F, it creates secure sessions using huge prime keys. However, many cloud apps will suffer as a result of this strategy.
Dodis et al. [21] investigated key-insulated symmetric key cryptography, which mitigates the harm caused by looping attacks on integrated cryptographic software. They highlighted the viability of symmetric key cryptography in key-insulated cryptography and created a kernel-based virtual machine environment as a proof-of-concept.
Sudha [22] investigated cloud security for data integrity, confidentiality, and authentication using a model that incorporates hyper crypto-encryption for both asymmetric and symmetric cryptographic algorithms as part of a data security paradigm for cloud computing..
Gampala et al. [23] investigated data security in cloud computing by using elliptic curve cryptography to implement encrypted digital signatures.
By solving equations over a ring of integers, Goswani and Singh [24] created an NP-complete class. The algorithm created increases public encryption agreements and can be utilised in a cloud computing service's server.
Even sophisticated techniques, such as FHE, are not enough to increase cloud privacy, according to Van Dijk and Juels [25]. This study's findings were remarkable for their resistance to cryptography's privacy leakage..
The repercussions of a hypothetical hostile cloud on cloud customers' sensitive data were examined by Rocha and Correria [26]. This is an intriguing research topic because many clients who connect to clouds may upload a variety of malware or viruses. Several customers have even uploaded zombies for use in Botnets. As a result, Rocha and Correria proposed using cryptographic operations to implement great privacy for each user.

Several cryptograph fields have been identified by Agudo et al. [28] as being attractive to cloud computing providers. To achieve sufficient protection for customer data in cloud computing, a cryptographic solution must attract the attention of a large number of cloud providers and produce a high value monitoring level.

To solve the security issue, Zhao et al. [29] investigated the development of a system for trusted data exchange over untrusted cloud providers. The created system may enforce data owners' access control policies and protect cloud storage providers against unwanted access and data authorization..
Atyero and Feyisetan [30] investigated the secure transport of data sessions to and from the cloud and found significant difficulties. This research provides a novel and effective security solution for cloud computing challenges. To solve major security concerns about cloud data access, Atyero and Feyisetan advocated using homomorphic encryption.
Jaatun et al. [31] created a cloud computing secrecy algorithm. The redundant array of independent net-storages (RAIN) for cloud computing was a key finding of their study. The RAIN method separates and distributes data into parts. The original data cannot be reassembled since the relationship between the scattered portions is kept confidential. Each part is far too short to reveal any useful information. RAIN protects the privacy of data saved in the cloud.

IV. DISCUSSION

Data control, the impact of software systems on organic resources, and the transfer of data access control to another are all challenges that have arisen as a result of cloud computing. We conclude that cryptography can be utilised for the following purposes based on the aforementioned literature review:

- Proofs of irretrievability.
- Homomorphic encryption.
- Private information retrieval.
- Broadcast encryption.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

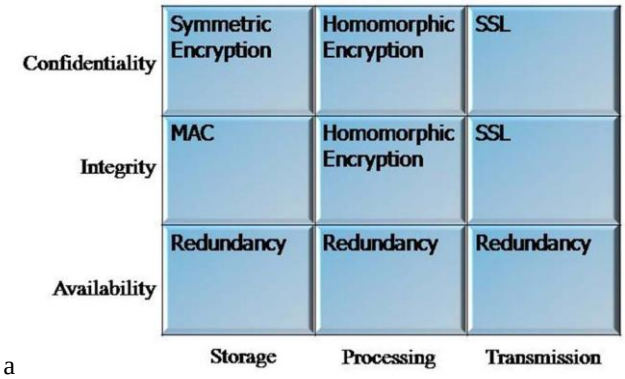
International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11653

- Knowledge and zero-knowledge proofs.
- Short signatures.

Thus, Fig. 5 Shown the concepts of cryptography usage over the three main security impression Confidentiality, Integrity and Availability (CIA).



a

Fig.5. CIA over cloud

As a result, the advantages of cloud computing have expanded throughout the backbone. However, the cloud computing sandwich would be incomplete without security algorithms, encryption, and policies. Furthermore, when many security implementations are made via multi-cloud, there will be another stumbling block in the form of performance. And how may thesis cryptography encryption items be manipulated with large keys at a lower cost, but the hint isn't finished yet? However, after security and performance, availability is crucial. As a result, the advantages of cloud computing have expanded throughout the backbone. However, the cloud computing sandwich would be incomplete without security algorithms, encryption, and policies. Furthermore, when many security implementations are made via multi-cloud, there will be another stumbling block in the form of performance. And how may thesis cryptography encryption items be manipulated with large keys at a lower cost, but the hint isn't finished yet? However, after security and performance, availability is crucial.

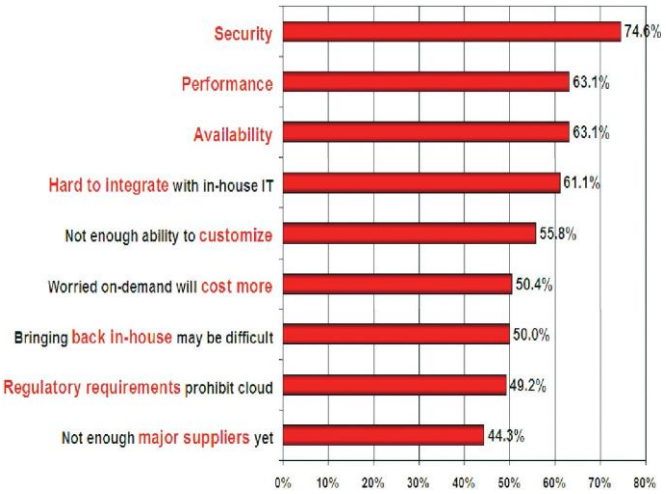


Fig. 6. Cloud usage vision

VII.CONCLUSION

Although there has been an advance in security in the cloud computing sector, there is no single solution that has been implemented cryptographically. A collaborative strategy for cloud computing could include a shared ownership of encryption algorithms and security policies. As a result, we consider that this progress is insufficient. However, based on our findings, we recommend that third-party boxes act as a gateway between clients and the cloud, acting as a crypto box, or that developers create programmes that act as an encryption/decryption mechanism, which could be built-in between clients and the cloud server as a cryptography secure session agreement.

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11653

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 JOURNALOF 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 andmethod," Google Patents, 2012.
[10] S. Bleikertz, S. Bugiel, H. Ideler, S. Nürnberger, and A.-R. Sadeghi, "Client-controlled Cryptography-as-a-Service inthe 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 inCloud 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.