EasyChair Preprint

№ 3050

# To Develop an Efficient Privacy Preserving Algorithm for Preserving the Privacy of the Cloud User's

Raghav Mittal and Areeba Kazim



March 26, 2020

# To Develop an Efficient Privacy Preserving Algorithm for Preserving the Privacy of the Cloud User's.

Raghav Mittal
Department of Computer Science and Engineering
Amity University,Noida
mittalraghav45@gmail.com

Areeba kazim
Department of Computer Science and Engineering
Amity University, Noida
aribakazim1995@gmail.com

***Abstract*— Abstract- Cloud computing provides insight to various aspects of business world and its ability to provide there exists a security threat, concern of data loss and data integrity and so these cheap and on demand network access and availability from any part of the world is what has led to its growth in a drastic way. Since the cloud services are available to everyone via internet connection become various aspects of concerns. We aim to focus on the security threats, privacy prevention and data privacy of the user. As all the confidential data is stored on the remote cloud servers hence the cloud service provider should maintain his trust from the client side .Although various steps have been taken and encryptions are used for data security still there are loopholes left which needs to be focused upon. Cloud computing relies on sharing of data, software and software based services. The few services offered by cloud include Infrastructure as- a- service (Iaas), Software as-a-service (Saas) and Platform as-a-service (Paas). We will get to know about how encryption works between the communication channels and an insight of cryptography model. We aim to focus on security of the cloud.**

***Keywords*— *Cryptography, Privacy prevention, Services, Security, Privacy, RSA Algorithm.***

## I. INTRODUCTION

Just as the word refers to Cloud means, the availability of the things anywhere and everywhere the same thing implies to the cloud we use in the Computer Science. The huge data centers of various companies are perfect examples of cloud computing such as Google drive, I Cloud and various others. There is no need of installing and maintaining the new hardware's as the maintenance is done by the service provider [1]. The cloud systems are blend of the virtualization and automation for creating an easy-to-consumer data center infrastructure service. The virtual hosting and cloud storage is being provided by cloud vendor. This is a basic model of public cloud.

The idea of using cloud reduces the hardware installation cost and maintenance describing is quality of being very cost effective. The on demand service is highly appreciated as it is scalable and the user pays for what he/she uses. Cloud refers to the on demand service access and the scalable property makes it more convenient for the users as they need not worry if they consumed their usage they still can access by paying extra. Since the user does not know where the data is stored and how the data is processed such as stored in which type of encryption, whether they have a backup of users data or not [2].

These factors lead to security concerns. Lack of security is the only hurdle in wide adoption of cloud computing and as the cloud is public in nature mostly various security issues arises. Few of the concerns are how the end users of cloud computing know that their information is not having any availability and security issues? Every one poses, Is their information secure[2]? .

## II. DEPLOYMENT MODELS

The cloud has been defined and divided according to the characteristics they posses and kind of service they provide. They are classified as-

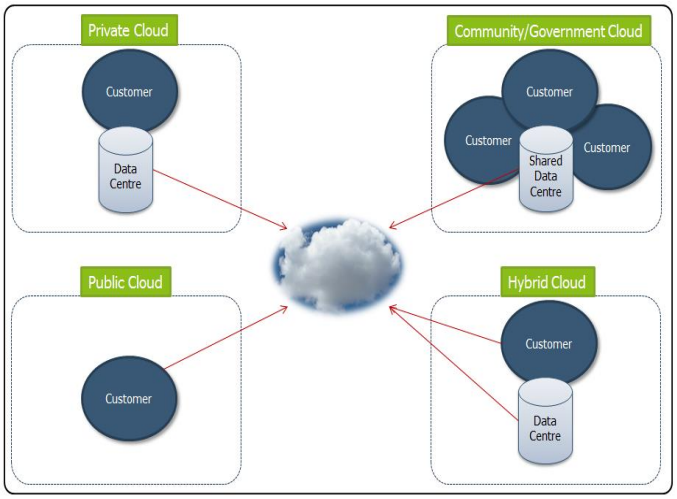


Fig 1.Cloud Storage

### A.PUBLIC CLOUD

This type of cloud is Open source and has the most security concerns because the services are being accessed by the people who don't have in depth knowledge about security. The data is created and stored on the third party servers. Public clouds have various advantages such as easy data access and its 24hours data availability. There is no need for the user to pay for the services used and the public clouds are scalable

and flexible to a great extent [4]. These clouds have few disadvantages which include data integrity and security threats are main concerns. They have lifted scope and the user cannot exceed the given accessibility permissions defined for public clouds [5].

### B.PRIVATE CLOUD

The private clouds have same architecture as that of the public cloud but they both have different technical points. These clouds have a business point of view and provide solution to the corporate or the individuals who purchase their services. These clouds have high customization facility available for their users and they have high level of security as they have paid service. The private cloud gives more access permissions to the users [6].

### C.HYBRID CLOUD

The hybrid clouds use concepts of combining both the public and private clouds. It consists least a combination of one public and one private cloud which is used in this communication. Since a combination of clouds is used for data transfer and storage these clouds are more vulnerable to security threats and data security is an issue, as the communication should be seamless [7][8].

### D.COMMUNITY CLOUD

These clouds are based on the interconnectivity between the private clouds. These clouds are built and operated specifically for a targeted group with aim of performing specific task [8]. These communities have similar cloud requirements and they aim to achieve their business objectives. This type of cloud service model provides a cloud computing solution to a limited number of individuals or organizations that is governed, managed and secured commonly by all the participating organizations or a third party managed service provider.

## III. SERVICES

In this section we shall discuss about various services of cloud. The cloud with its various advantages offers services which make it more suitable for meeting industrial needs[9][10].


Fig 2.Services of Cloud [8]

Iaas - The term Iaas stands for Infrastructure as a service. It provides virtual environment where the services has no need of buying the hardware and maintaining it. Here a cloud provider hosts the infrastructure components traditionally present in an on-premises data center, including servers, storage and networking hardware, as well as the virtualization or hypervisor layer[11].

Saas- This service mainly focuses on the developers and programmers. This service provides on demand computing and software delivery models [12].The provider gives customer the single copy of the software.

Paas-Platform as a service (Paas) is a cloud computing model in which a third-party provider delivers hardware and software tools -- usually those needed for application development -- to users over the internet [13].

## IV. SECURTY CONCERNS RELATED TO CLOUD

After seeing all the services and deployment models the main question comes are we safe? Is our data safely stored and encrypted? Is there any breach of data? These questions give rise and attract our interests on the security issue being faced in the cloud industry [13][14]. Here is a small discussion on it.

### Data Integrity

It is the most crucial point in the information system. Data integrity means protecting data from outside sources and unauthorized modifications [14]. The vendor is responsible to keep the data safe and intact so that the communication between the users is not interfered. We could deploy various security measures to prevent the integrity of the data as it builds the trust of the client [15]. In cloud computing a real concern is whether the data transferred to the end user is

tampered or not or whether it has been changed by any external means[16]. If the data has been tampered or changed in between the communication then a higher level of security must be implemented and the data should be recovered. Hence for the vendor it is really a challenge to send data in an unharmed way.

## Data Availability

The main purpose of the cloud is to provide easy access of data to the cloud users. The all time availability of the data should be provided to the user. The cloud companies should have the capability to provide the information in an easy accessible way. Users should be made aware as where their data is stored this increases the trust level of user [17]. The cloud vendor should make the client aware of the data safety and jurisdiction of the local laws. Since the data is to be available to hence it should be stored in proper databases and data centers should work with good interconnectivity. Hence the storage should be on reliable devices.

## Data storage

The data should be stored in the cloud servers with proper security and proper hardware's should be deployed for this purpose. The storage type can be physical servers with data being stored at multiple locations where the physical environment is provided by the proper companies. The data may be stored via distributed resources but still acts as one this is the main advantage of the cloud storage. Various copies of the data are also made up through servers and storage hardware's. By sharing storage and networks with many other users/customers it is possible for and sometimes because of criminal intent. Encryption should be applied at all the storage other customers to access your data [18][19]. Sometimes because of wrong actions, faulty equipment, a bug levels to ensure proper security.

*1) PREVENTION*

In this article we shall discuss on the encryption and decryption based protection of data. How the RSA algorithm works.

*2) CRYPTOGRAPHY*

The act of doing secure communication in the presence of third party in such a way that the data is not breached. The cryptography gives rise to encryption and then secure communication is done over the network. The diagram depicts use of two keys in asymmetric encryption.

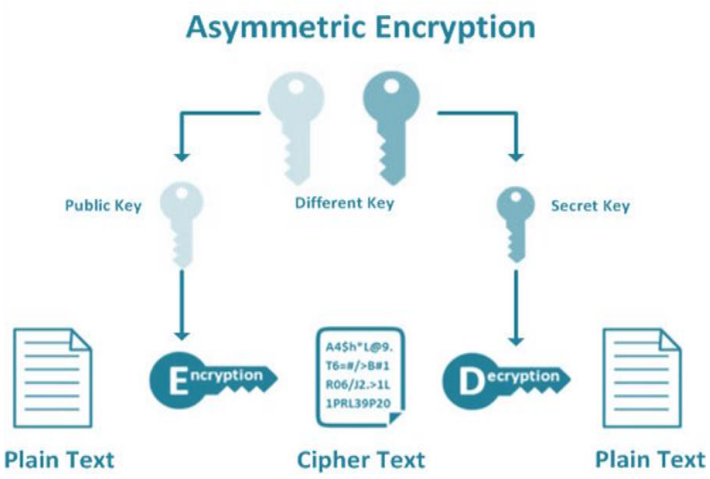


**Fig3. Process of Encryption and Decryption**

*3) ENCRYPTION*

The way of encoding the plain text into such a form that only the people who have authority to access can only understand it. The encryption is done with the help of an encryption algorithm depending upon the complexity of the problem the algorithm is deployed [17]. The hierarchy goes in this way: plain text which is encrypted using an encryption algorithm – a cipher – generates a cipher text that can be read only if decrypted in proper format. An authorized recipient can easily decrypt the message key provided by the developer hence restricting the access of the unauthorized user. This argument gives rise to 2 major forms of key encryption algorithm:

1. Symmetric Key algorithm
2. Asymmetric key algorithm

SYMMETRIC ALGORITHM

In this type of algorithm a single cryptographic keys are used for encrypting a plain text and decrypting of cipher text. The keys may be same or have slight difference going between the two keys. The key may be shared between multiple users as this type of encryption is used for the services provided by public cloud. Since the public cloud has a huge user base as compared to any other form of the cloud so it is not possible to generate a new key every time though the data of the user is secured[19].

ASYMMETRIC ALGORITHM

This algorithm uses a pair of shared key for encrypting and decrypting over the cloud network. Here the role of 2 keys comes into play. RSA key encryption is categorized under asymmetric key encryption which we will discuss.

### *RSA Algorithm*

This algorithm is used for public-key cryptography in asymmetric algorithm. It involves a pair of public key and a private key [19]. The public key encrypts messages and is common to all. Messages encrypted with the use of public key can be decrypted only by using the private key. In this verification process, the server implements public key authentication by using a unique digital signature with its private key [20]. The signature is then returned to the client. Then it verifies using the server's known public key.

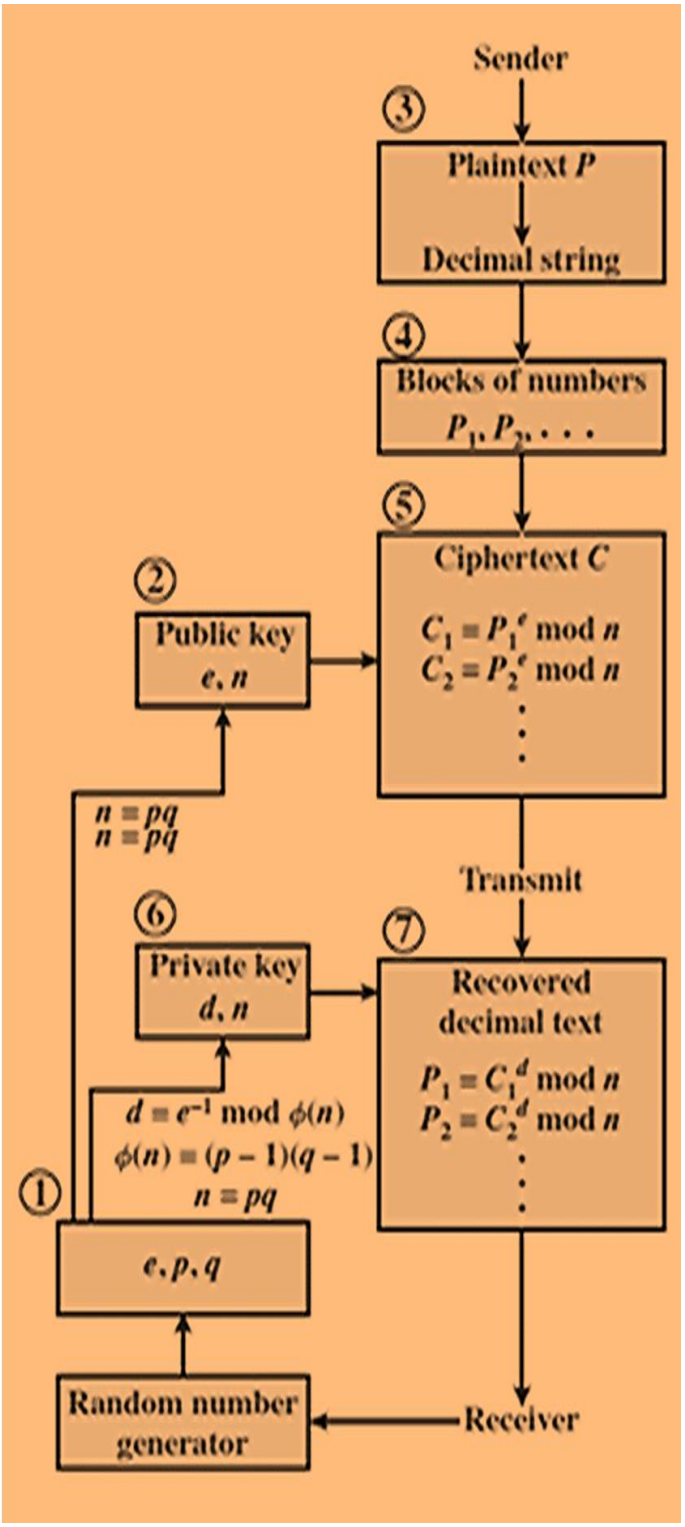


**Fig4.RSA Algorithm [20]**

The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could

be broken in the near future. But till now it seems to be an infeasible task.

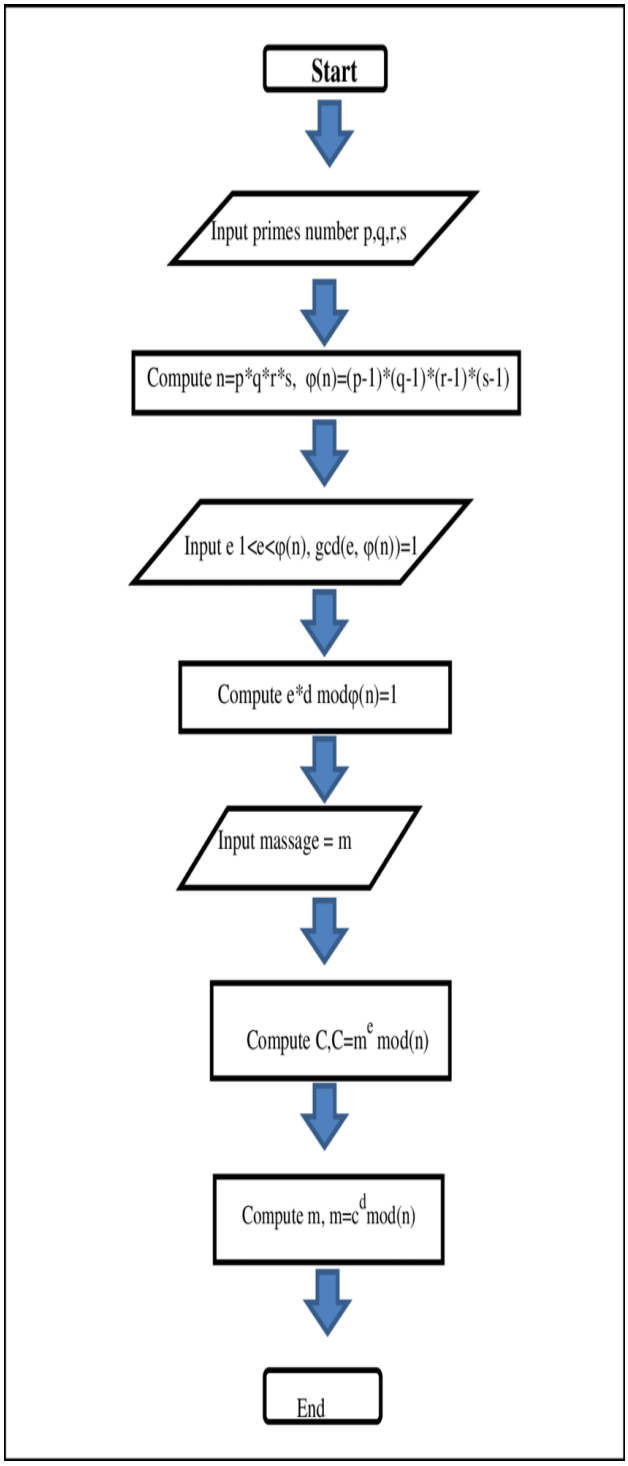


**Fig5.A simplified RSA [20]**

## V. RESULT

With increasing number of cloud users everyday more and more amount of data is being transferred over internet giving rise to the security concerns. Hence in this paper we discussed some of the data threats and how to deal with them. We briefed about how data can be compromised.

Various schemes have been discussed for preventing the data against cyber attacks which costs heavy losses to the corporations. Cloud user base works on trust between the two parties and breach of data is responsibility of both the sides. Using RSA algorithm which is based on public key cryptography throws some light on how data is handled. Data stored in huge servers works on virtualization techniques and is available in form of various kinds of cloud services. On the other hand cloud computing has really made data storage and handling easy and convenient through virtualization.

## VI.FUTURE WORK AND SCOPE

In digital world cloud provides interconnectivity between various organizations and corporate areas. And data is stored in local storage for security reasons. All companies are build on trust hence security is a major requirement in cloud computing and is a key are of concern. There are a various techniques which are being implemented for cloud security [20]. The future scope of cloud computing will have a combination of cloud based software products and on premises compute to create a hybrid IT solution in attempt to maintain balance of the scalability and flexibility associated with cloud and the security and control of a private data center. We should aim at developing more encrypted cloud security algorithms which should protect data when the data is not user's control. But we should also focus on the fast recovery of data if in case the data is tampered or the server crashes. Better versions of existing encryption techniques need to implemented such as that of RSA, DES, and AES.

## VII.CONCLUSION

Cloud computing is an emerging field in terms of next generation of IT technology. The only main issue faced by cloud is that of security and data breach. The real benefit is no maintenance of hardware is to be done and cost effectiveness [20]. No organizations would like to provide their information to the cloud database until the trust is built between the cloud service providers and consumers. Various research works have proposed techniques for data protection so as to attain highest level of data security in the cloud. This paper has surveyed various techniques about data security and privacy, focusing on the data storage and Use in the cloud. In situations where there is something relatively commoditized like storage as a service, they can be used interchangeably. This solves the issue of what to do if a Cloud Provider becomes unreliable or goes down and means the organization can spread the usage across different providers.

## VIII. REFERENCES

[1] S Renuga, S S K Jagatheeshwari, Efficient Privacy-Preserving Data Sanitization over Cloud Using Optimal GSA Algorithm, The Computer Journal, Volume 61, Issue 10, October 2018, Pages 1577–1588, https://doi.org/10.1093/comjnl/bxy067.

[2] On cloud security requirements, threats, vulnerabilities and countermeasures: A surveyKumar R. and Goyal R.Computer Science Review • 2019

[3] Wang, Jian & Zhao, Yan & Jiang, Shuo & Le, Jiajin. (2010). providing privacy preserving in Cloud computing. 2. 213 - 216. 10.1109/ICTM.2009.5413073.

[4] https://www.geeksforgeeks.org/how-to-solve-rsa-algorithm-problems/accessed on 12/08/2019.

[5] https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences/accessed On 13/8/2019.

[6] H. Zhu, R. Lu, C. Huang, L. Chen and H. Li, "An Efficient Privacy-Preserving Location-Based Services Query Scheme in Outsourced Cloud," in IEEE Transactions on Vehicular Technology, vol. 65, no. 9, pp. 7729-7739, Sept. 2016.doi: 10.1109/TVT.2015.2499791

[7] A reformed grasshopper optimization with genetic principle for securing medical data Annie Alphonsa M.M. and Mohana Sundaram N.Journal of Information Security and Applications • August 2019 • Pages 410-420

[8] Dyadic product and crow lion algorithm based coefficient generation for privacy protection on cloud George A. and Sumathi A.Cluster Computing • 16 January 2019 • Pages 1277-1288

[9] PSV-GWO: Particle Swarm Velocity aided GWO for privacy preservation of data Mandala J. and Sekhara Rao M.V.P.C.Journal of Cyber Security and Mobility • 2019 • Pages 439-466

[10] On cloud security requirements, threats, vulnerabilities and countermeasures: A surveyKumar R. and Goyal R.Computer Science Review • 2019 • Pages 1-48

[11] https://digitalguardian.com/blog/cryptography-cloud-securing-cloud-data-encryption/accessed on 16/08/2019

[12] https://www.researchgate.net/publication/274230804_Data_Security_and_Privacy_in_Cloud_Computing/accessed on 16/08/2019

[13] Identity-as-a-service: An adaptive security infrastructure and privacy-preserving user identity for the cloud environmentVo T.H., … +2 … , Furnell S.Future Internet • 1 May 2019

[14] Statista, Size of the cloud computing and hosting market marketworldwide from 2010 to 2020, URL https://www.statista.com/statistics/500541/worldwide-hosting-and-cloud-computing-market/, [Accessed on07-Jul-2018], 2017

[15] S. Subashini, V. Kavitha, A survey on security issues in service deliverymodels of cloud computing, J. Netw. Comput. Appl. (ISSN: 1084-8045) 34(1) (2011) 1–11, http://dx.doi.org/10.1016/j.jnca.2010.07.006N. Khan, A. Al-Yasiri, Identifying cloud security threats to strengthencloud computing adoption framework, Procedia Comput. Sci. (ISSN: 1877-0509) 94 (2016) 485–490, http://dx.doi.org/10.1016/j.procs.2016.08.075.

[16] A. Singh, K. Chatterjee, Cloud security issues and challenges: A survey, J.Netw. Comput. Appl. (ISSN: 1084-8045) 79 (2017) 88–115, http://dx.doi.org/10.1016/j.jnca.2016.11.027.

[17] G. Ramachandra, M. Iftikhar, F.A. Khan, A comprehensive survey onsecurity in cloud computing, Procedia Comput. Sci. (ISSN: 1877-0509)110 (2017) 465–472, http://dx.doi.org/10.1016/j.procs.2017.06.124.

[18] L. Coppolino, S. DAntonio, G. Mazzeo, L. Romano, Cloud security: Emerg-ing threats and current solutions, Comput. Electr. Eng. (ISSN: 0045-7906)59 (2017) 126–140, http://dx.doi.org/10.1016/j.compeleceng.2016.03.004.

[19] .Yang,Y.Sun,Q.Wu,Batchattribute-basedencryptionforsecureclouds,Information (ISSN: 2078-2489) 6 (4) (2015) 704–718, http://dx.doi.org/10.3390/info6040704

[20] .W. Felten, M.A. Schneider, Timing attacks on web privacy, in: Pro-ceedings of the 7th ACM Conference on Computer and CommunicationsSecurity, in: CCS '00, ACM, New York, NY, USA, 2000, pp. 25–32, http://dx.doi.org/10.1145/352600.352606.