

# An efficient and secure data storage in cloud computing using modified RSA public key cryptosystem

International Journal of Electrical and Computer Engineering (IJECE)

*International Journal of Electrical and Computer Engineering (IJECE)*

## Cite this paper

Downloaded from [Academia.edu](#) 

[Get the citation in MLA, APA, or Chicago styles](#)

## Related papers

[Download a PDF Pack](#) of the best related papers 

## An efficient and secure data storage in cloud computing using modified RSA public key cryptosystem

Y. Kiran Kumar<sup>1</sup>, R. Mahammad Shafi<sup>2</sup>

<sup>1</sup>Department of Computer Science, Bharathiar University, Coimbatore, India

<sup>2</sup>Bharathiar University, Coimbatore, India

---

### Article Info

#### Article history:

Received Apr 16, 2019

Revised Aug 17, 2019

Accepted Aug 29, 2019

---

#### Keywords:

Cloud data storage

Cloud service models

Data security

Modified RSA

Public key cryptosystem

RSA

---

### ABSTRACT

Cloud Computing is the ability to improve the utility or train new human resources without investing in new infrastructure, or add capabilities to existence without the latest software licensing. It expanded the capabilities of Information Technology (IT). From the past few years, cloud computing has developed from a good business concept in the best rising sectors of the IT industry. But more information on individuals and companies was put in the cloud, and concerns began to think about how secure the cloud environment was. Despite cloud surrounding structures, enterprise users still do not want to expand their business in the cloud. Security reduces the growth of cloud computing and continues to spread the market with complexity with data privacy and data protection. The security of cloud computing has constantly been an significant aspect of improved quality of service from cloud service providers. Data storage in the cloud has a problem related to data security. However, cloud computing construct many new security challenges which have not been well examine. In order to ensure that the user's data in the cloud is secure, we have proposed an effective mechanism with a distinctive feature of data integrity and privacy. This paper focusing on problems relating to the cloud data storage techniques and security in virtual environment. We recommend a method for providing data storage and security in cloud using public key Cryptosystem, which uses the concept of the modified RSA algorithm to provide better security for the data stored in the cloud.

Copyright © 2020 Institute of Advanced Engineering and Science.  
All rights reserved.

---

### Corresponding Author:

R. Mahammad Shafi,  
Research Spervisor, Bharathiar University,  
Coimbatore, India,  
Email: rmdshafi@gmail.com

---

## 1. INTRODUCTION

Cloud Computing has many unique features that make it very valuable. Different types of services can be easily accessible from cloud computing. Cloud Computing services provide client-specific applications and Data storage through dedicated cloud servers. That means there are no data and applications on the computer used by the client. Only the operating system and the cloud computing service will be the only application. The client will have to access the applications and data so that he can directly access from cloud server. This whole process is called cloud computing. Using cloud computing does not have the risk of software, crash, and data loss. Moreover, the client-utilized device also works faster. With virtualization technologies, cloud computing uses more efficient resources [1]. Cloud Computing services are growing and expected to expand in the future. The physical server runs many virtual machines and operating systems. Cloud Computing has a facility to use computing resources directly through the Internet. Computing source may be a combination of software or hardware, or both, and computing resources will be released in the form of Internet services. A service allows the user to access the computing

resource. Services operate on a remote server and users access the interface as a browser. Cloud computing stores data stored on a user's remote cloud server [2]. Information technologies take new waves in order to change civilizations. Computing significantly expanded, making the database more robust.

Cloud computing detects briefly that cloud computing services offer client-specific applications and data storage through dedicated Web servers. In Cloud Computing all data is stored on a web server. There are no data and applications on the client-utilized computer [3]. Only the operating system and the cloud computing service will be the only application. Client Applications and data are accessible to get cloud servers directly from cloud servers. There is no risk of software, crash and databases using cloud computing, the client-utilized device also works faster.

## 2. CLOUD COMPUTING DEPLOYMENT MODELS

In Cloud Computing each model has a unique value proposition, which provides a line improvement provider for the business and provides customer service option. The following is some of the major or popular cloud operation models.

- a. Private Cloud: Private Cloud infrastructure is controlled by a company or a third party and only maintains the requirements of the company.
- b. Public Cloud: Public Cloud infrastructure is available to a large organizations or general public and owned by the vendor who provides cloud services.
- c. Community Cloud: Community Cloud infrastructure is a shared community that has operated by one or more organizations and supports the same services.
- d. Hybrid Cloud: Hybrid Cloud infrastructure is a combination of two or more different cloud infrastructures like private, public or community clouds, but portability of data and applications provided by standard technology.

## 3. CLOUD COMPUTING SERVICES

The wide range of services offered by cloud computing organizations can be categorized into three basictypes:

### 3.1. Software as a service (SaaS)

Many users allow access to the application when SaaS services provide better accessibility and active functionality. SaaS services provide focused business operations. The cloud resource administrator creates controls regarding users' access to applications.

### 3.2. Platform as a service (PaaS)

User configuration under PaaS does not use the applications and facilities provided by the cloud provider. Cloud storage options are available to use cloud needs. The model pre-runner manages all cloud computing designs. It provides support for applications and services and provides computational resources through the host platform.

### 3.3. Infrastructure as a service (IaaS)

This environment can include hardware, operating systems, network connectivity and other IT resources. The IT resources provided by IaaS are generally not pre configured, placing the administrative responsibility directly upon the cloud consumer. The user of the PaaS dedicated API makes it possible to organize the activities of the server hosting engine to run and reproduce the environment based on user requests. Each provider is based on its API related key capabilities, the app developed for each particular group provider is not moved to another cloud host, but its API is excluded based on its related key capabilities. There are attempts to extend simple programming designs with cloud capabilities. In Cloud environment data is not stored on the user's computer but stored in the third parties cloud storage. The Cloud Computing infrastructure allows its resources to be accessed between users, servers and can openly access data/file stored in the cloud server. Due to this open access factor, one person's files or data is used by other users of the cloud, resulting in more or less dangerous to treat data or files. Once intruders have access to data, its abuse is a major threat. Intruder destroys the actual data or break off the communication. Cloud service providers provide critical security over files and data that require much attention to security. One of the most common problems in the cloud is that the person does not control the data storage space. Cloud Service Provider provides a cloud user provided resource allocation and scheduling facility, when processed when required to protect files/data. To defeat this problem, security in the cloud server should be effective.

#### 4. DATA SECURITY USING ENCRYPTION

Security is a key element in wide range of areas like network security, data security and user access mechanisms. In Cloud Computing one of the major area is data security, encryption mechanisms, data resiliency and replication, data availability and integrity are some of the popular methods to provide data security in cloud computing. In these methods we have used encryption method by using RSA and Modified RSA algorithms. In cloud-based data transmissions most commonly used protocol is HTTPS, which uses SSL/TLS underlying protocol. Most of the Transport Layer Security implementations used by RSA algorithm because it is the chief asymmetrical encryption cipher.

Generally Cloud Services has more harm than the intra network services and also additional security problems arise on virtualization and outsourced resources. The major Cloud Security problems are raised based on the selection of Cloud Service Model and runtime of the applications. To identify the security problems on the cloud environment we have to analyze the following steps:

1. Identify the resource: Identify which type of resource (Data/Applications or Services) to deploy on the cloud environment.
2. Identify the access level of the resource: Identify the risks that are associated on the resource related to availability, privacy, unauthorized access and loss of data.
3. Identify the deployment model: Cloud deployment models are private, public, community and hybrid. Identify which type of deployment model is appropriate for your resource.
4. Determine the delivery model: Different cloud delivery models are available such as IaaS, PaaS and SaaS. Identify which type of delivery model is suitable for your IT resource.
5. Evaluation of Cloud Provider: Users need to assess the system to know where data is stored and how data is transferred in and out of the cloud environment after identify resources offered by a cloud provider.

Infrastructure is provided by IaaS, Frameworks for application development, manage structures and transactions provided by PaaS and an Operating Environment with applications, effective user interface and management provided by SaaS. From the existing service models IaaS has the least integrated functionality so it requires minimum security but SaaS has more integrated functionality so we require more security [4].

SaaS is delivery model for shared cloud services that can be located as commercialized products hosted by clouds. In this model cloud consumer is given access the cloud service contact, but not any underlying IT resources or implantation details. The PaaS cloud delivery model enables a cloud provider to offer a preconfigured environment that cloud consumers can use to build and deploy cloud services and solutions, even though with decreased administrative control. A Cloud Consumer is accessing a ready-made PaaS environment. IaaS cloud delivery model offers cloud consumers a high level administrative control over “raw” infrastructure-based IT resources. A cloud consumer is using a virtual server with in an IaaS environment. Cloud consumers are provided with range of contractual guarantees by the cloud provider, pertaining to characteristics such as capacity performance and availability.

#### 5. RSA ALGORITHM

RSA authentication and the identity of service provider over insecure communication medium. Cracking the RSA encryption is at most as difficult as factoring huge numbers [5, 6]. The RSA algorithm involves three steps [7, 8]:

1. Generation of Key
2. Encryption by using Public Key and
3. Decryption by using Private Key.

Select two different prime numbers  $p$  and  $q$ .

The integer's  $p$  and  $q$  should be generated at randomly because of security.

compute  $n = p * q$ ;

compute  $f(n) = (p-1)(q-1)$

choose  $e$  such that  $e$  is relatively prime to  $f(n)$  and less than  $f(n)$ .

find out  $d$  such that  $de$  congruent modulo 1 ( $\text{mod } f(n)$ ) and  $d < f(n)$ .

Public key =  $\{e, n\}$ , Private key =  $\{d, n\}$

Cipher text  $c = \text{message } e \text{ mod } n$

Plain text  $p = \text{ciphertext } d \text{ mod } n$

## 6. MODIFIED RSA MODEL

Figure 1 show the encryption and decryption using MDRSA.

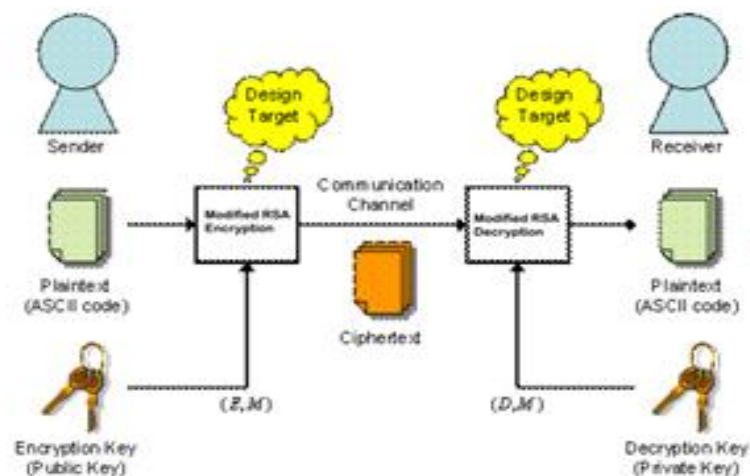


Figure 1. Encryption and decryption using MDRSA

We divide the program into 3 parts

1. plaintext + publickey1 --> ciphertext1
2. ciphertext1 + publickey2 --> ciphertext 2
3. ciphertext1 + private key --> plain text

In the majority cases the problem of RSA is breakable as of simply calculation of keys based on  $N$ , because it is the only product of two prime numbers,  $N$  can be easily noticeable. Once the value of  $N$  is recognized, an intruder can recover the keys and crack the system. The most important modifications which build the system is capable and secure are considered in the modified RSA Model [9, 10].

Modified RSA algorithm is performed by following way:

1.  $n1 = p \times q$
2.  $n2 = r \times s$
3.  $N = n1 \times n2$
4.  $ph = (p-1)(q-1)(r-1)(s-1)$
5.  $e = e1 \times e2$
6. Calculate  $e1$  and  $e2$  and multiply two values ( $e1 \times e2$ ) or calculate  $e$  and divide  $e$  into  $e1$  and  $e2$  then we get two encryption dan one decryption.

The modified RSA Model generates randomly four large prime numbers  $p$ ,  $q$ ,  $r$  and  $s$ . There are three components consisting in public key generation  $e$ ,  $f$ ,  $N$  where  $e$  and  $f$  are at random generated and also three components consisting in private key generation  $d$ ,  $g$ ,  $N$  where  $d$  and  $g$  are randomly generated [11, 12]. In customized RSA model more complexity number is  $N$ . In public and private key generation  $N$  is the same value, an intruder with the information of  $N$  cannot find out the values of four prime numbers which are essential for finding the value of  $N$  and consequently  $e$  and  $f$  [13, 14].

## 7. RESULTS AND DISCUSSIONS

Key Size: [1024]

Generated prime numbers  $p$ ,  $q$ ,  $r$  and  $s$

$p$ :

[DBB0B0485D335DF044F4EDD18415D5A43BAF2C9FB8A99BE5347E910138D19AF24788AF77801DE68E47BBB85AA839DC374A539B3AE6F8449389BDC5FCEF3F6298C06C17264BA809FD7EC50FE0D9A7753EF8F2C30216046-----]

$q$ :

[96D0AF060D3116D4686A5156CD44FF53B647376816B3F34D00BB7A0DAF048627A49494716E41DA822D5734976DA6FB5EBA062CC913758E6208E93D6D7E4320331CE85C841E031095B0FDBA7730BD85F3CFD8FB9B1CAD15C-----]

r:

[8DD21B80761BBF6C8C0DB42F70CBB9DE0962DC0C19DE32D77830B6856BE09E5158C302C94F98212982086BB09DF8098064F848B8D4401D544E37C76D0B1C7033B431037FEAD1557296626188B20DF1756E2B7A7191B2C72D4FB7A-----]

s:

[9FEBECA150EB7E87E6F63C8E20E19F8112379CA8BF0FA7F474EB0BC6662BE29C2CD50B22330EB0CA0D6BC9FE3288A275A706845CC518C989F2FBC1FD3001C18FBAE3BFA3505912B72D411A5DCDCA18A941255699432494C1D2162-----]

Public Key pair n and E

Generated Value of N:

[2CCA47C6672AA889B2FBB67F1D71B6C4884A8CB7B0EBBD5FFEB52507C83DA918A509C858A38937CDC68DDB55C20FE7F44C9195048F5E00447C66734D9094BDC164F067C68AD7470FF784282FBD32E123309C469E360EDF9-----]

Generated Value of E:

[D12E253C6B9A2D1C4DAF5890FB3D5ACBB8CBE7736E37AC70B3AEFEEC5AEF2B2AC2484C9E769AF1D44831A9DDE0EF2E767269FFD07F99854B4A0583EAF4457B7907B2F50EBC55C4A34656E4AA62190477ECEF5BA8FF8CD0D01DB-----]

Private Key pair n and D

Generated Value of N:

[2CCA47C6672AA889B2FBB67F1D71B6C4884A8CB7B0EBBD5FFEB52507C83DA918A509C858A38937CDC68DDB55C20FE7F44C9195048F5E00447DA64677C28F24FD8069389D8B6CFC66734D9094BDC164F067C68AD7470FF784-----]

Generated Value of D:

[1A9A8F639F9776D55E9C0C79E00728BDE804E7A9C513613E1C5197FD519E78A030719A670543923597D602D5F1A9F8DA1192D491A73B68D94F47F27396FD95135BFD88EA9EB1A17A11D776A3D471D5F6394632FA100BA7D4AFE883A3-----]

Please enter message (plaintext):

This is secret information

Generated Cipher text:

[532076F90468DA03C7696D357210A2DDB35444D25D764A1D705535B320F25029DB786E7DF8114C4C4D877A271318D41823AA1B7647DACB1E2A9B9A866F951F740056732D758DF177FA41B280D3764BF6D5B320242210A9BF1E667-----]

Execution time for encryption in milliseconds: 3087.0078

Generated Cipher text1:

[1FAA52CC64E4A85AA9CD083C1116BC9BF07D90A8FD19A7C12C8C7FBEA0E976F788D5BA532F2046D6D873E8031672A8A1A8B02772AB7F12679A647E1288417CF45B9E4AE6AE65D8DB49B6A6E3A3C77E2B07B714E8BE2C56C7AF5-----]

Execution time for decryption in milliseconds: 3087.0078

Recovered plaintext: [This is secret information]

Figure 2 show time consumption for different key sizes by key generation using RSA and MDRSA Algorithm.

Key Size (bits)	RSA (ms)		MDRSA (ms)	
	Encryption time	Decryption time	Encryption time	Decryption time
128	8.388608	5.24288	12.582912	12.582912
256	14.68006	12.582912	74.4489	68.15744
512	134.2177	134.2133	536.8709	536.8709
1024	536.8709	402.6532	3087.0078	3087.0078
2048	3489.661	3355.443	26172.457	26575.11

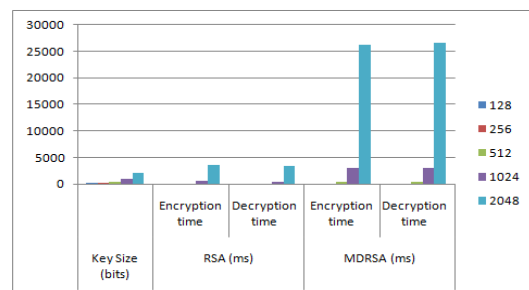


Figure 2. Time consumption for different key sizes by key generation using RSA and MDRSA Algorithm

The RSA and Modified RSA models represent the encryption and decryption time in milliseconds based on key sizes from 128 bits to 2048 bits. We recommended that Modified RSA with key size 1024 bits will be a optimize solution which make balance between speed and security from the reaming key size values [15, 16].

## 8. PERFORMANCE EVALUATION

The proposed Modified RSA (MDSA) algorithm is examined on varying bit sizes of input. Performance of original RSA algorithm by Rivest, Shamir, and Adleman [17, 18] are shown in Table 1. Also the performance of Modified RSA (MDSA) scheme in terms of encryption time and decryption is shown in Table 2. Comparing the above tables, it can be concluded that the time of key generation of Modified RSA (MDSA) is higher than that of RSA. The higher key generation time of Modified RSA (MDSA) can be seen as an advantage by the fact that the time to break the system is high because of the extra complexity added. Figure 3 shown the encryption time comparison between RSA and proposed Modified RSA (MDSA) scheme [19, 20]. It illustrates that, for the lower bit length of prime numbers, two algorithms consume the almost identical amount of time. But with the increase of bit length, the difference between curves rises rapidly [21, 22].

Table 1. Encryption time comparison using RSA and MDRSA Algorithms

Key Size (in bits)	Encryption time in ms (RSA)	Encryption time in ms (MDRSA)
128	0.19	0.68
256	0.36	1.48
512	0.57	3.2
1024	1.72	7.8
2048	3.33	21.92
4096	11.18	56.88

Table 2. Decryption time comparison using RSA and MDRSA Algorithms

Key Size (in bits)	Decryption time in ms (RSA)	Decryption time in ms (MDRSA)
128	0.29	2.9
256	0.98	14.28
512	5.3	87.96
1024	26.19	446.34
2048	130.84	2472.72
4096	1116.26	19983.38

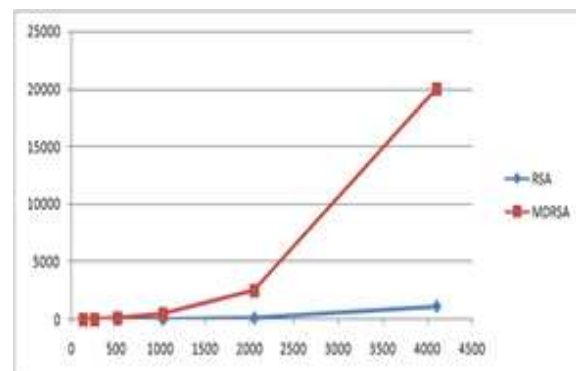
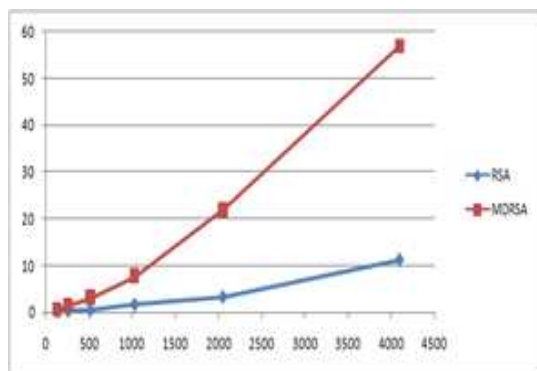


Figure 3. Encryption and decryption time comparison using RSA and MDRSA Algorithms based on key size

Figure 3 illustrate the encryption and decryption time comparison between RSA and proposed Modified RSA (MDSA) scheme. We recommended that Modified RSA with key size 1024 bits will be a optimize solution which make balance between speed and security from the reaming key size values [23, 24]. With the increase of bit length, the difference between curves elevates rapidly at key size 2048 and 4096, it can be easily seen that encryption and decryption times are higher than RSA. The increase in time is adaptable because it increases the security to a great extent in the proposed Modified RSA (MRSA) method [25].

## 9. CONCLUSION

This manuscript has proposed a structure to provide confidentiality protection to the data stored in cloud environment. The modified RSA scheme used to protect the data in such a way that no reveal of data on cloud. Thus, in our projected work, only the approved user can access the data using the private key can be correctly decrypted. If some unauthorized users gets the data by chance or intentionally if he/she captures

the data also, he/she can't decrypt it and get back the original data from it. With the help of this new security model which is modified RSA Public Key Cryptosystem, we can improve the security flaw of existing data security model in cloud environment and thereby guarantee the data security in cloud environment. In this modified RSA algorithm verification is more secure than RSA algorithm.

## REFERENCES

- [1] Sosinsky, "Understanding Cloud Security," Cloud Computing Bible Sosinsky/Cloud, 2011.
- [2] B. A. Forouzan, "Cryptography and Network Security," Tata McGraw Hill Education Private Limited, New York, 2010.
- [3] M. B. Mollah, *et al.*, "Next generation of computing through cloud computing technology," *2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, 2012.
- [4] Thomas E., "Cloud Computing, Concepts, Technology & Architecture," Pearson Publication, 2014.
- [5] M. A. Islam, *et al.*, "A Modified and Secured RSA Public Key Cryptosystem Based on "n" Prime Numbers," *Journal of Computer and Communications*, 2018.
- [6] I. G. Amalarethinam and H. M. Leena, "Enhanced RSA Algorithm with Varying Key Sizes for Data Security in Cloud," *2017 World Congress on Computing and Communication Technologies (WCCCT)*, Tiruchirappalli, pp. 172-175, 2017.
- [7] Y. Pachipala, *et al.*, "Data Security in Cloud using RSA," *2013 Fourth International Conference on Computing Communications and Networking Technologies (ICCCNT)*, 2013.
- [8] P. Garg and V. Sharma, "An efficient and secure data storage in Mobile Cloud Computing through RSA and Hash function," *International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, 2014.
- [9] A.V.N. Krishna, "Chapter 16 A Randomized Cloud Library Security Environment," IGI Global, 2014.
- [10] R. Biswas, *et al.*, "A fast implementation of the RSA algorithm using the GNU MP library," IIIT – Calcutta.
- [11] S. Sharma, "RSA algorithm using modified subset sum cryptosystem," *Computer and Communication Technology (ICCCCT)*, pp. 457-461, 2011.
- [12] A. Mousa, "Sensitivity of Changing the RSA Parameters on the Complexity and Performance of the Algorithm," *Journal of Applied Science, Asian Network for Scientific Information*, vol. 5, pp. 60-63, 2005.
- [13] M. A. Islam, *et al.*, "A Modified and Secured RSA Public Key Cryptosystem Based on "n" Prime Numbers," *Journal of Computer and Communications*, vol. 6, pp. 78-90, 2018.
- [14] M. Thangavel, *et al.*, "An Enhanced and Secured RSA Key Generation Scheme (ESRKGS)," *Journal of Information Security and Applications*, 2015.
- [15] R. S. Dhakar, *et al.*, "Modified RSA Encryption Algorithm (MREA)," *2012 Second International Conference on Advanced Computing Communication Technologies*, Rohtak, pp. 426-429, 2012.
- [16] H. M. Sun, *et al.*, "Dual RSA and Its Security Analysis," *IEEE Transactions on Information Theory*, vol. 53, pp. 2922-2933, 2007.
- [17] T. C. Segar and R. Vijayaragavan, "Pell's RSA Key Generation and Its Security Analysis," *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, Tiruchengode, pp. 1-5, 2013.
- [18] M. J. Wiener, "Cryptanalysis of Short RSA Secret Exponents," *IEEE Transactions on Information Theory*, vol. 36, pp. 553-558, 1990.
- [19] A. H. Al-Hamami and I. A. Aldariseh, "Enhanced Method for RSA Cryptosystem Algorithm," *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, pp. 402-408, 2012.
- [20] Y. Li, *et al.*, "Design and Implementation of an Improved RSA Algorithm," *2010 International Conference on E - Health Networking Digital Ecosystems and Technologies (EDT)*, Shenzhen, vol. 1, pp. 390-393, 2010.
- [21] A. Chhabra and S. Mathur, "Modified RSA Algorithm: A Secure Approach," *2011 International Conference on Computational Intelligence and Communication Networks*, Gwalior, pp. 545-548, 2011.
- [22] B. Swami, *et al.*, "Dual Modulus RSA Based on Jordan-totient Function," *Procedia Technology*, vol. 24, pp. 1581-1586, 2016.
- [23] R. Patidar and R. Bhartiya, "Modified RSA Cryptosystem Based on Offline Storage and Prime Number," *2013 IEEE International Conference on Computational Intelligence and Computing Research*, Enathi, pp. 1-6, 2013.
- [24] R. L. Rivest, *et al.*, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," *Communications of the ACM*, vol. 21, pp. 120-126, 1978.
- [25] K. Govinda, *et al.*, "Data Security in Cloud using Blowfish Algorithm," *International Journal for Scientific Research & Development*, vol. 2, 2014.



**BIOGRAPHIES OF AUTHORS**

**Mr. Y.Kiran Kumar, M.C.A, (Ph.D)**, he received his Master of Computer Applications from Sri Venkatesra University, Tirupati. He is Pursuing Ph.D from Bharathiar University, Coimbatore. He is having more than 10 years of teaching experience, Currently he is working as a Assistant Professor in the department of M.C.A in Sree Vidyanikethan Engineering College, Affiliated by JNTUA, Ananthapuramu, India. His areas of research interests include Web Technologies, Service Oriented Architecture and Cloud Computing.



**Dr. R. Mahammad Shafi, M.C.A, M.Tech, Ph.D** He received his Ph.D from University of Allahabad, Allahabad. He is having more than 20 years of teaching experience. His areas of research interests include Software Engineering, Software Testing and Quality Assurance. He has published papers in refereed journals and conference proceedings in these areas. He has been involved in conferences and workshops as a Committee member, organizer and Session Chair.