A Comparative Analysis of Encryption Techniques and Data Security Issues in Cloud Computing

N. Hemalatha
M. Phil Scholar
St. Joseph's College
Tiruchirappalli, India

A. Jenis
M. Phil Scholar
St. Joseph's College
Tiruchirappalli, India

A. Cecil Donald
Research Scholar
St. Joseph's College
Tiruchirappalli, India

L. Arockiam
Associate Professor
St. Joseph's College
Tiruchirappalli, India

ABSTRACT

Cloud computing has been seen as the next generation architecture of IT enterprise. The cloud paradigm advantages and its potential for decreasing costs and reducing the time for a service that favours towards security issues. Cloud Computing is an aggregation of IT services that offered to the customer based on leasing. Though a large number of security issues are addressed, still some are not addressed and several algorithms are proposed for security issues. This paper presents a perspective of cloud computing technologies, essential characteristics, classifications, delivery models and various encryption mechanisms. A comparative study made on several encryption techniques are used for maintaining the confidentiality in the cloud. Finally, the major data security issues present in cloud computing are discussed.

Keywords

Cloud Computing, Confidentiality, Encryption, Data Security Life Cycle

1. INTRODUCTION

Cloud Computing is a set of IT services provided by various service providers. The term cloud has originated from the internet and cloud computing is a platform that gives people the opportunity for sharing resources, services and information among the people globally. In general, cloud computing has different definitions offered by several important organizations. One of the standard definition National Institute of Standard and Technology (NIST) [1] defined cloud computing as *"a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., Network, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"*. Security and privacy are always the major concerns in cloud computing. According to Gartner's survey, 70% of respondents think that the recent CTO of cloud computing without the utilization of the primary reasons is that there is data security and privacy concerns [2]. Google Apps is the best example of cloud computing where everyone can access their applications on Google data centers through a web server [3]. Security is categorized into two shells such as protecting the assets and protecting the data. Storing data in the cloud have many benefits which reduce hardware cost and improve storage reliability. In cloud computing, data security problem was not resolved entirely. Some of the security parameters are availability, authentication, confidentiality and integrity. Users don't know where the information will be stored in the cloud. Most users care about the confidentiality of their information. Confidentiality is the important parameter in all cases of deployment. Confidentiality can be categorized into two characters, namely weak confidentiality and strong confidentiality. Weak confidentiality means only authorized users and cloud providers get the meaningful data from cloud storage. Strong confidentiality means cloud providers cannot access the data. For example confidential business information, government secret information, etc. Cloud computing provides an efficient storage for computer storage and call back the cloud users sensitive data. Using symmetric encryption techniques, the user's data are encrypted before storing into the cloud storage.

This paper is organized as follows: Section 2 explains the Essential Characteristics of Cloud Computing and Section 3 presents the Classifications of Cloud Computing. Section 4 presents Delivery Models of Cloud Computing. Section 5 elaborates various Encryption Techniques for Data Security in Cloud Computing. Section 6 lists out the current Data Security Issues in cloud computing and finally, Section 7 concludes the paper.

2. ESSENTIAL CHARACTERISTICS OF CLOUD COMPUTING

- ***On-demand Self Service:*** Cloud consumers expect on demand services from the cloud environment. The service provider must allow self-service access according to their request. So that customers can request customized, pay and use services without the intervention of human operators.
- ***Broad Network Access:*** Cloud resources are globally available and utilized through a standard mechanism that promotes the user by heterogeneous platform.
- ***Resource Pooling:*** The providers of cloud pooled the resources together and serve multiple clients using multiple tenant models.
- ***Rapid Elasticity:*** The cloud will be flexible and scalable to suit consumer business needs. Consumers can easily add or remove users, software features, resources, etc.
- ***Measured Service:*** Cloud computing resource usage can be measured, controlled and reported providing transparency for both provider and consumer of the utilized service.

3. CLASSIFICATION OF CLOUD COMPUTING

Based on the customer service and their usage, the cloud can be classified as public, private, community, and hybrid.

3.1 Public Cloud

Public or external cloud infrastructure is available to the general owned by an organization for selling cloud service on pay-per-use basis. Some examples of public cloud are Google App Engine and Windows Azure services platform.

3.2 Private Cloud

Private or internal cloud infrastructure is maintained and controlled by a single organization. Some examples of private cloud are Sun Cloud, Google App Engine, IBM Blue clouds, etc.

3.3 Community cloud

Community cloud is another type of private clouds. Cloud infrastructure is shared by several organizations, typically with shared concerns. It may be managed by a group of organizations or third party on/ off premises.

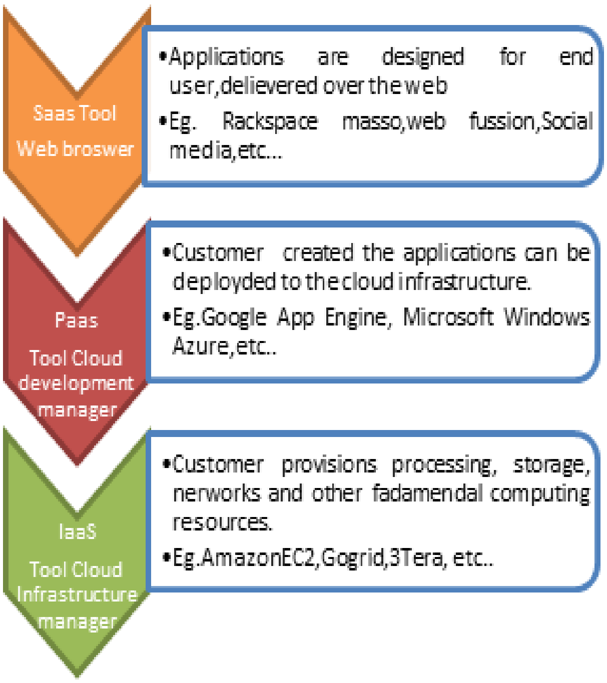
3.4 Hybrid Cloud

Cloud infrastructure consists of two or more public, private or community clouds. The purpose of hybrid cloud is to provide extra services and resources to customers to serve their demands.

4. DEPLOYMENT MODELS IN CLOUD COMPUTING

Services are offered by cloud providers can be grouped into three categories. Figure 1 explains the cloud delivery models.

- Software as a Service (Saas)
- Platform as a Service (Paas)
- Infrastructure as a Service (IaaS)


Saas Tool
Web broswer
Paas
Tool Cloud development manager
IaaS
Tool Cloud Infrastructure manager

- Applications are designed for end user,delievered over the web
- Eg. Rackspace masso,web fussion,Social media,etc...

- Customer created the applications can be deployded to the cloud infrastructure.
- Eg.Google App Engine, Microsoft Windows Azure,etc..

- Customer provisions processing, storage, nerworks and other fadamendal computing resources.
- Eg.AmazonEC2,Gogrid,3Tera, etc..

Figure 1. Cloud Delivery Models

4.1 Software as a Service (SaaS)

Software is provided to the cloud customer as a service. Over the web the SaaS applications are delivered to end users [4]. SaaS is offered by Google Apps [5], Salesforce.com [6], Social media, Gmail is software as a service of Google, etc. Advantages of Saas is scalable, flexible pricing, portability, user-friendly.

4.2 Platform as a Service (Paas)

Platform as a Service means a way to rent hardware, operating system and network capacity over the internet. The platform is provided to the cloud customer as a service. Google App Engine [8], Microsoft Windows Azure [9] is the popular example of paas. Advantage of paas is Google minimizing developers, maintained customization and configuration.

4.3 Infrastructure as a Service (IaaS)

Infrastructure as a Service means just building a home from beginning, it consists “on demand” to internet connection, space with the flexibility to increase or decrease server capacity [7]. The IaaS cloud example is Amazon EC2 [10], Go grid, 3tera, etc... The advantage of IaaS is a Cloud solution cost scales according to use.

5. ENCRYPTION TECHNIQUES FOR DATA SECURITY IN CLOUD

Encryption Techniques are used for securing the sensitive information [11]. There are two different encryption techniques are used commonly.

Symmetric Key Encryption uses Single key is involved in data security. Both sender and receiver use the same key to encrypt and decrypt.

Asymmetric Key Encryption uses two keys are involved. The receiver has a secret key which is private and another key public which is published to everyone.

Generally, Classical Encryption algorithms categorized into two principles.

- Substitution Cipher (replaces one character with another)
- Transposition Cipher (transpose or reorder the characters).

Homomorphic encryption concept origin from esoteric world of abstract algebra. Homomorphic means same shape or same effect on two different sets of objects can be transformed. The fully homomorphic encryption means (FHE), that there are no limitations on what manipulations can be performed [12].

The following section analyses the various symmetric encryption techniques, which effectively handle large amount of data.

5.1 Classical Substitution Cipher Algorithm

Padmapriya et al [13] have proposed a method for providing the inverse of Caesar Cipher that supports more security for the data compared with earliest Caesar Cipher. The main scope of their paper is a new level of data security solution with encryption using ASCII full characters, which is important for designing the complete security solution. Caesar Cipher is replacing the letter three places down in the alphabet. For example “COME” is a plain text which will be converted into “FQOH” as cipher text. But this cipher can be broken by brute force attack because at the end there are only 25 possible available options of key.

Sastry et al [14] proposed playfair cipher which has encrypt multiple letters. They used a square matrix of 5x5 alphabetical letters are arranged in an appropriate manner. The user can select the key and place it in the matrix. The user can select a key and place it in the matrix. The remaining letters of the English alphabet from the key are then one by one placed in the matrix of playfair cipher. The plain text is broken into pairs and if a pair ha same alphabet is separated by introducing a filler letter with ‘x’.

5.2 Fully Homomorphic Encryption

Maha tebaa et al [15] proposed an application of a method to execute operations on encrypted data without decrypting them, which will provide us with the same results after calculations as if the authors have worked directly on the raw data. Homomorphic Encryption method is able to perform operations on encrypted data without decrypting. Homomorphic Encryption systems are used to perform operations on encrypted data without knowing the private key (without decryption), the client is the only holder of the secret key. In their paper, a new concept of security which enables providing results of calculations on encrypted data without knowing the raw data on which the calculation was carried out, in respect of the data confidentiality. The improvement of the complexity of the Homomorphic encryption algorithms and compares the response time of the requests to the public key.

Huda et al [16] proposed fully homomorphic encryption (FHE) allows a user that does not have the secret decryption key to compute any result of the data. The author focused technique is based on a FHE algorithm with key delegation to ensure data confidentiality, authentication, integrity and availability of multi-level hierarchical order. Their proposed framework solution is the using of homomophic cryptography with Attribute Based Encryption.

5.3 Cryptography, Encryption Technique

Sugumaran et al [17] discussed techniques that are implemented to protect data and propose an architecture to protect the data in the cloud. Their architecture was developed to store data in the cloud in encrypted data format using cryptography technique which is based on a block cipher. Their proposed architecture is based on cryptography algorithm, which is secure for data storage. This architecture has been designed for data security using block based symmetric cryptography, having better speed for storing the data. Their algorithm improved encryption of data secured by interesting the symmetric layer and using this technology is efficient for storing the user’s data in the cloud.

Prashant et al [18] have proposed a “Three way mechanism” ensures all the three protection scheme of authentication, data security and verification at the same time. Their proposed architecture to make use of digital signature and Diffie Hellman key exchange with AES algorithm to protect confidentiality of data stored in the cloud. Their proposed mechanism makes it tough for hackers to crack the security system, thereby protecting data stored in the cloud.

- Diffie Hellman keys in exchange.
- Digital Signature used for authentication
- AES encryption algorithm is used to encrypt or decrypt user’s data file.

In cloud storage environment to avoid data modification, they used two separate servers are maintained, one for encryption process known as computing platform and another one known as a storage server for storing user data.

5.4 Cloud DES Algorithm

Neha Jain and Gurpreet et al [19] have proposed Data security in cloud computing using the DES algorithm. This Cipher Block Chaining system is to be secure for clients and server. The security architecture of the system is designed by using DES cipher block chaining, which eliminates the fraud that’s occurring today with stolen data. The data which are sent, being intercepted and replaced has no danger. The system with encryption is acceptably secure, but that the level of encryption has to be stepped up, as computing power increases. Results in order to be secured the communication system between the modules are encrypted using a symmetric key. The author proposed that the cloud data security must be considered to analyze the data security risk, the data security requirements, deployment of security functions and the data security process through encryption. The main contribution of their paper is the new view of data security solutions with encryption, which is important and can be used as reference for designing the complete security solution.

Monikandan et al [20] have described an encryption algorithm to address the security and privacy issue in cloud storage to protect the data from unauthorized access. Data can be attacked in two ways. An insider attack is an administrator having the possibility to hack the user’s data. Outsider attack is third party can access the user’s data. The Author proposed a symmetric encryption algorithm to protect the data stored in cloud storage from the unauthorized access. Their proposed technique is converting plain text into the corresponding ASCII code value of each alphabet and the key value ranges between 1 to 256. This technique improves classical encryption techniques by integrating substitution cipher and transposition cipher. Symmetric encryption has the speed and computational efficiently to handle encryption of large volumes of data in cloud storage. Their proposed algorithm is used to encrypt the user data in cloud storage and it can’t be accessed by administrators or attackers. The main contribution of this paper is a comparison between various Symmetric Encryption algorithms are compared based on its techniques, description, concepts, security, issues addressed.

Table 1. Comparison Techniques of Existing Encryption Algorithms

Author	Techniques Used	Description	Concepts Used	Security Applied On	Issues Addressed
Padmapriya et al	Inverse Caesar Cipher	Classical Substitution Cipher Same key used for Encryption & Decryption	ASCII full characters (256 characters)	Cloud customer and Cloud provider side	Data Security and Privacy
Sastry et al	Playfair Cipher	Classical substitution Cipher. Same key used for Encryption &	5x5 matrix and Alphabetic characters used	Cloud customer and Cloud provider	Data Security and Privacy

		Decryption		side	
Maha et al	Fully Homomorphic Encryption	The private key is used for Encryption (without Decryption)	Cryptosystem based on fully Homomorphic Encryption	Cloud provider side only	Data Security
Huda et al	Fully Homomorphic Encryption	The private key is used for Encryption (without Decryption)	Electronic Health Records classify based on PI (Personally Identifiable information)	Cloud Customer and Cloud Provider side.	Data confidentiality, Authentication, Availability and Integrity.
Sugumaran et al	Block based Symmetric Cryptography	Symmetric layer inserted for encrypting the secure data using a symmetric algorithm	The private key concept is used between sender and receiver	Cloud Customer side	Data Security and Privacy
Monikandan et al	Classical Encryption	Both Substitution and Transposition. Same key used for encryption and Decryption	Palin text is converted to ASCII code value, key range between 1 to 256	Customer's side only	Data Security and Privacy
Neha Jain et al	DES Algorithm	The same key is used for Encryption and Decryption	Cipher Block Chaining mode	Both Cloud customer and Cloud provider	Data Security

6. DATA SECURITY ISSUES IN CLOUD COMPUTING

Data Security means protecting data from unauthorized access, modification or destruction. In the cloud model, service provider is responsible for maintaining the data security. Recently, technology has focused on only one stage for a data security life cycle, which is process manage from creation to destroy. Figure 2 explains the data security life cycle and the phases in it.

- **Create**: This phase is the generation of new digital content in client or server in the cloud.
- **Store**: This phase occurs simultaneously after the creation process, therefore storage of data occurs in the repository or stored in multiple nodes.

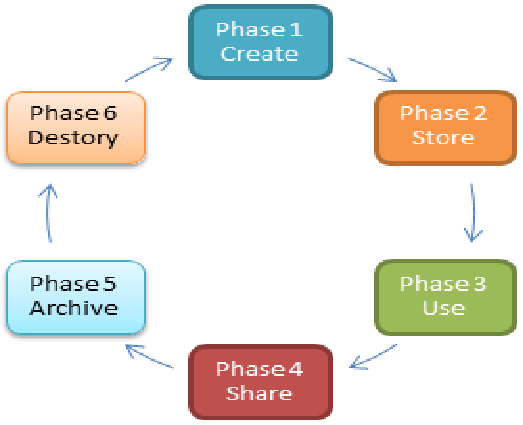


Figure 2. Data Security Life Cycle

- **Use:** This phase uses the data in the repository for various processes.
- **Share**: In this phase, the transmission of data occurs between customers and the partners.
- **Archive:** In this phase, stored data is utilized for future use.
- **Destroy:** This phase will permanently remove the data in the repository.

Data security threats can be classified into internal threats and external threats. Internal threats, mainly come from an insider attack because cloud service providers and users, are the main reason for these threats. External threats, mainly come from outside attack because data can be accessed from third party. The attacker can steal the user's personal data. [21]. There are Six types of major issues [22], while discussing data security in the cloud.

- Data Authentication
- Data Privacy and Confidentiality
- Data Integrity
- Data Location
- Data Availability
- Data Storage, Backup and Recovery

6.1 Data Authentication

A user may gain access within a LAN by entering a cloud identification and password, which may be affirmed by a cloud authentication mechanism. If the authentication mechanism validates the certification, the user identification and password are stored locally for subsequent authentication requests. The authentication mechanism may be applied in both domain and Workgroup LAN and may function in parallel with other users who may have a LAN or client credentials which may not be authenticated from the cloud.

6.2 Data Privacy and Confidentiality

Once the clients outsource data to the cloud there should be assurance that data is accessible to only authorized users. The cloud computing service provider should make secure the customer personal data is well protected from other service provider's and user. Authentication is the best solution for data privacy because service provider must make sure who is accessing the data and who is maintaining the server; so that the customer's personal data is protected. The cloud customer must be guaranteed that data stored in the cloud will be confidential [22].

6.3 Data Integrity

Data Integrity means data is complete and consistent. The data stored in the cloud may suffer from damage during integration operations. The cloud provider must make the client aware of what particular data are outsourced to the cloud, the native and the integrity mechanisms put in place [22].

6.4 Data Location

The cloud users did not know where the data will be hosted and in fact, their users want to know the location exactly. It requires a contractual agreement between the users that data should stay in a particular location.

6.5 Data Availability

Data provided by the customer is normally stored in different servers often placing in different locations or in different clouds. Data availability becomes a major legitimate issue as the availability of corrupted and relatively difficult servers.

6.6 Data Storage, Backup and Recovery

The cloud users decide to move their data to the cloud provider should ensure adequate resilience storage systems. The process of recovering and backing up data is simplified. The cloud providers will store the data in several places across many independent servers.

7. CONCLUSION

Cloud computing is a versatile technology, widely studied in recent years. The providers and the clients must make sure that the cloud is safe from all the internal threats, external threats and mutual understanding between the customer and provider when it comes to the security of cloud. The major issues in cloud computing is data security and it has many aspects like confidentiality, Integrity, surveillance, reliability, availability, Security, anonymity, telecommunications capacity, government and backup & recovery. But the most important issue in data security is security and privacy for protecting the data in cloud storage. This paper analyses the importance of the data security in the cloud. Reason for choosing symmetric encryption algorithms are effective to handle encryption for large amount of data, and effective speed of storing data in the cloud. In this paper, table 1 explains the comparison among various encryption techniques used in the cloud.

8. REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing", September 2011.

[2] Anwar J. Alzaid, Eng. Jassim M. Albazzaz, "CLOUD COMPUTING: AN OVERVIEW", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 9, September 2013.

[3] Donald, A. Cecil, S. Arul Oli, and L. Arockiam. "Mobile Cloud Security Issues and Challenges: A Perspective." International Journal of Electronics and Information Technology (IJEIT), ISSN (2013): 2277-3754.

[4] Maneesha Sharma, Himani Bansal, Amit Kumar Sharma, "Cloud Computing: Different Approach & Security Challenges", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[5] Sales force. Salesforce CRM applications and software solutions. http://www.salesforce.com/eu/crm/products.jsp

[6] Google, Google Apps. <http://www.google.com/apps/>.

[7] Sarvesh Kumar, Jahangeer Ali, Ashish Bhagat, Jinendran P.K, "An Approach to Creating a Private Cloud for Universities and Security Issues in Private Cloud" International Journal of Advanced Computing, Vol. 36, Issue 1, ISSN: 2051- 0845, 2013.

[8] Cecil A Donald and L Arockiam. Article: Securing Data with Authentication in Mobile Cloud Environment: Methods, Models and Issues. International Journal of Computer Applications 94(1):25-29, May 2014. Published by Foundation of Computer Science, New York, USA.

[9] Microsoft. Microsoft Windows Azure. <http://www.microsoft.com/windowsazure/>.

[10] Amazon. Amazon Elastic Compute Cloud (EC2). <http://aws.amazon.com/ec2/>.

[11] Padmapriya and Subhasri,"Cloud Computing: Security Challenges & Encryption Practices", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, ISSN: 2277 128X, March 2013.

[12] C. Gentry, "Computing Arbitrary Functions of Encrypted Data", ACM, Vol. 53, Issue 3, March 2010, pp. 97-105.

[13] Padmapriya, Subhasri," Cloud Computing: Reverse Caesar Cipher Algorithm to Increase Data Security", International Journal of Engineering Trends and Technology (IJETT), Volume 4, Issue 4, 2013.

[14] V.U.K. Sastry, N. Ravi Shankar and S. Durga Bhavani, "A Generalized Playfair Cipher involving Intertwining, Interweaving and Iteration", International Journal of Network and Mobile Technologies, pp 45-53, 2010.

[15] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI "Homomorphic Encryption Applied to the Cloud Computing Security" Proceedings of the World Congress on Engineering, London, U.K. ISBN: 978-988-19251-3-8 ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online), Vol 1, July 4 - 6, 2012.

[16] Huda Elmogazy, Omaima Bamasak," Towards Healthcare Data Security in Cloud Computing", IEEE 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013).

[17] Sugumaran, BalaMurugan. B, D. Kamalraj," An Architecture for Data Security in Cloud Computing", IEEE World Congress on Computing and Communication Technologies 2014.

[18] Prashant Rewagad, Yogita Pawar," Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", 2013 IEEE International Conference on Communication Systems and Network Technologies.

[19] Neha Jain and Gurpreet Kaur," Implementing DES Algorithm in Cloud for Data Security"VSRD-IJCSIT, Vol. 2 (4), 2012, 316-321.

[20] L. Arockiam, S. Monikandan," Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.

[21] Xiaojun Y, Qiaoyan Wen," A View about Cloud Data Security from Data Life Cycle", IEEE 2010.

[22] Parsi Kalpana and Sudha Singaraju, "Data Security in Cloud Computing using RSA Algorithm", International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

9. AUTHORS BIOGRAPHY

N. Hemalatha is doing M. Phil research in the Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India. She had attended several National and International Workshops and Conferences. Her area of research is Cloud Computing. Her area of interest is Networks Security, Software Engineering and Web Technologies.

A. Jenis is doing MPhil research in the Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India. She had attended several National and International Workshops and Conferences. Her area of research is Cloud Computing. Her areas of interest are Networks Security, Software Programming and Web Developing Technologies.

A. Cecil Donald received his Masters in Software Engineering from Anna University, Chennai, India. He has one year experience in IT industry as a Software Developer. Currently, he is a Ph.D. research scholar in the department of Computer Science at St. Joseph's College (Autonomous), Tiruchirappalli affiliated to Bharathidasan University, India. His main area of research is Mobile Cloud Computing. He has published several papers in the International Journals and also he has atteneded several national and international conferences and workshops.

Dr. L. Arockiam is working as Associate Professor in the Department of Computer Science, St.Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India. He has 25 years of experience in teaching and 18 years of experience in research. He has published more than 187 research articles in the International & National Conferences and Journals. He has also presented 2 research articles in the Software Measurement European Forum in Rome. He has chaired many technical sessions and delivered invited talks in National and International Conferences. He has authored 3 books. His research interests are: Cloud Computing, Big Data, Cognitive Aspects in Programming, Data Mining and Mobile Networks. He has been awarded "Best Research Publications in Science" for 2009, 2010 & 2011 and ASDF Global "Best Academic Researcher" Award from ASDF, Pondicherry for the academic year 2012-13 and also the "Best Teacher in college" award for the year 2013 & 2014.