Mitigating Cloud Security Threats Using Public-Key Infrastructure

Disha H. Parekh and R. Sridaran

Abstract Cloud computing is a very huge entity, as a technology, in recent era, evolving at a very rapid pace. There is a wide progress from mainframe computers toward the client/server infrastructures, including cloud computing deployment models with rudiments from autonomic computing, grid computing, and utility computing. This transition has brought tremendous effects on areas of information security and communications. These effects are majorly viewed positively, but there are some critical issues to be concerned. Due to this major transition toward cloud, various risks and challenges, identified and unidentified, have been discovered weakening the traditional security approaches. For this reason, that paper is aimed twofold: First to evaluate the requirements for cloud security and second is to propose a viable solution which would eradicate major potential threats. The model introduced in this paper will help to demolish network-related threats that arise due to trusted third party. The proposed solution will also enhance cryptography with Public-Key Infrastructure and helps in mitigating security threats. The solution presents a broad way of trusting services that realizes any security threats.

Keywords Cloud computing security · Confidentiality · Integrity Availability · Trusted third party · Information security · Public-key infrastructure · Mitigating security threats · RD model · Scramble Unscramble · AES · DES · 3DES

D. H. Parekh (✉) · R. Sridaran
Faculty of Computer Applications, Marwadi Education Foundation's Group of Institutions, Rajkot, Gujarat, India
e-mail: disha.hparekh213@gmail.com

R. Sridaran
e-mail: sridaran.rajagopal@gmail.com

D. H. Parekh
Computer Science Department, Bharathiar University, Coimbatore, Tamilnadu, India

M. U. Bokhari et al. (eds.), *Cyber Security*, Advances in Intelligent Systems and Computing 729, https://doi.org/10.1007/978-981-10-8536-9_17

1 Introduction

Computing has bloomed and expanded horizontally and vertically with lots of innovations in the field. There has been a wavy graph with a nudge in the information and communication age. The computing era initiated with mainframe computers, traversing toward minicomputers to personal computers later and now we have reached to the most noteworthy era, i.e., cloud computing era. Cloud computing services are offered by identified Cloud Service Providers (CSP) across the globe. The CSP is considered to be simply an extension from Internet Service Provider (ISP) and Application Service Provider (ASP). At the very initial level, ISP 1.0 was implemented where Internet was provided locally to the institute. Later it got transformed to ISP 2.0 and ISP 3.0, where now the Internet services were available globally and users were able to connect with telecommunications and other service providers thru associated data centers. These further got evolved to ASP (ISP 4.0), where not only the computing infrastructure but also specialized applications were provided with a greater ease. But considering the problem of ASP where only dedicated infrastructures were implemented, a newer version of ISP, ISP 5.0, called CSP got evolved, where the computing infrastructure along with applications are available on a shared basis. Cloud computing characterizes a model transition—a transfer from product-based computing to a service orientated computing [1]. The US National Institute of Standards and Technology has defined that cloud computing is a technology that facilitates well-situated, need-based network admission to a communal group of computing resources, e.g., servers, networks, applications, and offerings that can be quickly given and free with negligible management attempt or service supplier interaction [2]. The cloud encourages ease of use and is collected of five necessary distinctiveness, three delivery models, and four deployment models [3]. Services offered by cloud computing are supplied with dynamism to the customer who owns their data on cloud. As per their demand and their need, the customer can easily access the data from cloud, as it is shared across the network, from any location at a very high speed. Apart from this, cloud also provides a very greater space for each individual to store data. Its benefits like multi-tenancy, i.e., sharing of resources at the network level, high scalability, elasticity, and pay-as-you-go facility have made cloud computing a promising and swiftly budding model.

These elementary taxonomies are usually known as the “SPI Model”, where it stands for Software services, Platform services, and Infrastructure services respectively [4].

- **Software as a Service (SaaS)**

An application hosted for its clients and who can use the services offered via the Internet is generally what SaaS does. A customer does not sustain or support the software; rather the software provider will only take care of its support and maintenance. Moreover, customers do not make any upgradation in the software

and do not require integration of other systems also. The provider only does the patching and necessary improvements. SaaS provides clients with network-based access to the commercially available software which is kept centrally.

- **Platform as a Service (PaaS)**

The second type of delivery model is PaaS, which supplies the necessary resources that are required to create applications and offerings online, with no need of downloading or installing any software. It includes services like the integration of web services, integration of database, scalability, protection, designing, testing, deployment, and hosting.

- **Infrastructure as a Service (IaaS)**

The last service model, IaaS, is the succeeding kind of service in which the hardware or the computing infrastructure is provided to the clients to put their data or applications on network. The infrastructure provided can be scaled up and down on demand, dynamically. Additionally, it even provides the feature of multi-tenancy on the same infrastructure. It is in other terms also known as Hardware as a Service (HaaS).

Regardless of the above service models exploited, there are four models that are deployed and implemented for cloud with derived disparities which need address specific requirements.

- **Public Cloud**

In this type of cloud, the service is obtainable by the general public or to any bigger organization. The cloud provided, is usually under the ownership of an organization that sells cloud services.

- **Private Cloud**

Over here, the cloud is open only to the single client, or a solitary organization. These types of cloud can be supervised either by the organization or any third party. It varies in 2 different forms, i.e., off-premise and on-premise. In off-premise, the cloud used is generally managed by any third party while in on-premise; the cloud is managed and owned by the organization that uses it.

- **Community Cloud**

In community cloud, the cloud is mutually used in numerous organizations and it supports an explicit community that has shared anxieties. It could be under the supervision of the organizations or of an intermediate party and may be situated on-premise or off-premise.

- **Hybrid Cloud**

This cloud is a combination of more than one cloud, i.e., private, public, or community which will exist as exclusive entities but are leaped mutually by the proprietary skill that allows data and application transportability.

The cloud computing security and related work done on security issues with either encryption technique or cryptography is mentioned in the first half. The next part describes the needs for cloud computing security with respect to Confidentiality, Infrastructure, and Availability (CIA) is discussed. This paper has also proposed a model that shows the use of DES algorithm in encrypting and decrypting process but involving scrambler and unscrambler. The proposed model ensures all major needs that cloud security requires. It enhances integrity assurance and confidentiality as well as the availability of data on cloud.

2 Related Work

It is observed that a large amount work has been carried out in the vicinity of cloud security. A major portion of the work focuses on the reliability verification the saved data in the cloud. Tangowan et al. [6] have depicted cloud computing security anxieties that are specifically related to security of data and privacy-based guard issues which has remained as a chief restraint for the implementation of services provided by cloud computing. They have offered with summarizing but thorough analysis on data security and privacy protection issues. But the disadvantage is that it does not show any practical implementation of the security policy or mechanism.

Somani et al. [7] state that in cloud computing problems like data security, file system, backup, and host security persists to a greater extent. They have projected a notion of the digital signature with the use of RSA algorithms to encrypt the sensitive data while shifting it over the network. This technique has tried to solve the problem of authentication and confidentiality. But as observed, the problem of integrity still persists.

Similarly, Rafique et al. [8] have shown a secure data transfer based on identity in cloud using a method called Group Digital Signature (GDS). In this, a group manager will commune with the service giver by using a secret key that will get produced by the Diffie–Hillman key exchange algorithm. Group manager obtains the member public key of all the users in the group. The user in the group sends the data to the cloud server and will sign the message with the assigned (d, n) private key. This message is acknowledged by the group manager who authenticates the group member and then gathers the necessary detail and further attaches the secret group id and sign and sends it to the cloud provider. Cloud provider will authenticate the message and will allow the encrypted message to be stored in private cloud. But as observed, one needs to trust the group manager, which might not be feasible at every instance [5].

Moreover, Fernandes et al. [9], has shown in their paper that security related to data in the cloud can be assured with the use of digital signature with help of CFX_MF algorithms. In this digital signature is used for the verification and non-repudiation of the message, where the uniqueness of sender and the reliability of the message are preserved. According to the paper, the integrity check over the cloud computing is performed by an intermediate party which inspects the data from client and hauls out the request of unauthorized user. Some researchers do not trust the third party as there is no guarantee of mutual and equal trust.

After surveying various papers, and flaws with the usage of encryption techniques in the papers, this paper is aimed to focus on guaranteed cloud security model. This model will use Data Encryption Standard (DES) algorithm with scrambling and unscrambling of data and is also ensuring the mechanism to assure data integrity and authentic data availability at the end once the encrypted data is decrypted.

3 Cloud Computing Security

Securing data on the web involves recognizing exceptional threats and challenges which necessarily has to be attended with greater impact by applying proper countermeasures. Eventually, the required security services and controls are set up with the typical systems engineering procedure in order to efficiently amalgamate the defense controls with the information systems practical and equipped requirements, plus other significant system requirements like reliability, maintainability, and supportability [10]. Usually, the architecture of cloud computing provides a single data center for data storage and computation [11]. There can be various security benefits in utilizing the cloud environment. But, a single malfunctioning should not be alleged for any data loss. It generally is very difficult to track down the security measures in a cloud environment. The current cloud service providers have introduced and placed many complicated methods and trained staff for sustaining their systems. Due to this, there are various security benefits like data centralization, data backup, incident response, logging, etc., available. Though it shows the presence of many security features, cloud computing still addresses major key security issues and challenges, like data segregation, usage of compromised servers, certificates and auditing security, investigating an illegal undertaking, and many more.

Cloud computing has become a most important development in IT. Enterprises should acclimatize to the diversifications it brings to maximize the return on investment. To assist organizations worldwide, International System Audit and Control Association (ISACA) has identified critical issues which need operational methods like effectively organizing risks, being transparent with the third party about the enterprise policies, handling myriad regulations and adapting competently [12]. In spite of several measures and steps for cloud security, the cloud has exclusive features that involve endangering evaluation in fields like availability

issues, data integrity, reliability problems, data recovery, and privacy and auditing, as stated in Gartner [13].

Cloud computing, thus, as concluded, has a huge number of security issues and challenges [14]. An elaborated record of security threats on the basis of the deployment and service models of cloud computing is presented and discussed in detail in [15]. Security, in general, to technology, is broadly standardized for evaluation of data systems security, focusing on three central goals of CIA, essentially known as, Confidentiality, Integrity, and Availability.

- **Confidentiality**

Confidentiality refers the access of restricted data only to authorized users and ceasing access of such protected data from unauthorized users. Confidentiality aims at authentication procedures like user-ids and passwords that solely recognize data users and sustaining procedures that hamper each recognized user's get access to the system's resources. But as there is augmented the quantity of parties, devices, and applications occupied on cloud, the threat compromised data grow substantially as the multiple access points come into existence. Such an increase in data usage leads to problems with multi-tenancy, applications security, data remnants, and privacy [16].

Cloud service providers usually are using a weak authentication mechanism that involves username and password and the access controls, i.e., authorization, is at a very coarse level, which results in significant security threats. To address these security threats and to answer the cloud protection, in essence, there is a use of encryption technique [17]. Encryption of data is carried out based on encryption algorithm and is dependent on key strength. The encryption carried out even depends on the cloud service providers; for example, EMC provides encryption facility to the customer data while Amazon's S3 does not provide any kind of encryption to customer data but instead customer's before uploading the data can encrypt the data on their own.

The encryption of data for the purpose of providing confidentiality to customer data primarily involves use of encryption algorithm. There are many encryption algorithms present but not all are fashioned equal [18]. Cryptographically, many algorithms are insufficient to provide the desired security. Algorithms that are evaluated by formal standard bodies like NIST or informally by the cryptographic community must be used. Next, the key length for encrypting data must be considered. It is essential to know that larger the key length, stronger is the encryption. For the NIST-approved algorithms like 3 DES (Triple Data Encryption Standard) minimum length should be of 112 bits, which will be shown in the proposed model.

- **Integrity**

Integrity is the next security aspect required for confidentiality. Integrity simply means that consumer assets can be customized only by the authenticated users and in an authorized way only. When it comes to data storage, maintaining data

integrity aspect is the obvious requirement. Data integrity ensures that no illicit or illegal modification, deletion, or fabrication of data is allowed and originality of data remains intact [19]. By keeping a check on the unauthorized access, organization attains greater confidentiality in terms of data integrity. Moreover, integrity also helps in accountability of data modification, data deletion or any constructed data, to find the potential source of such intrusion.

Data encryption is a solution for confidentiality but there should be a mechanism to assure and verify the data that is decrypted by the recipient. This is taken care of data integrity which uses message authentication codes tagged with the encrypted data. These message authentication codes work as a hash function which will ensure that the data that gets decrypted in the original sent message of the sender [20].

- **Availability**

The huge accessibility computing community has pursued a mantra that no particular source of failure should be observed, yet the administration of a cloud examine by a lone company is, in fact, a distinct point of failure [21]. Availability refers to every entity that comes when we talk about cloud. It targets the availability of data in cloud, states the availability of the cloud service provider, system availability and even talks about the availability of network level security mechanism to ensure data security. Hence, availability is not only about data presence in the cloud. Network is now getting highly congested and, therefore, need to assure clients that the data will be available to them dynamically at any point of instance.

System availability involves the ability of system to continue with functioning in a proper and accurate manner even when there is any kind of authority misbehaves noticed. In spite of any security breach is identified, system should be able to carry its operations as though normal. Cloud services show a severe reliance on the resource infrastructures and network accessibility at all times [22].

Business critical applications generally rely on continuous and constant delivery of services without a gap of any time. A simple service outage only for few minutes can have a serious impact on the productivity of the enterprise. It can also result in customer dissatisfaction and service-level disobedience. According to the Cloud Computing Incidents Database (CCID) [23], which trails cloud service outages, chief cloud service providers have undergone downtime ranging from just minutes to hours. Moreover, relying on the rigorousness of the occurrence and the extent of the exaggerated infrastructure, outages may involve all or a few of clients. During a cloud service commotion, harmed clients will not be in condition to contact the services and in a few cases can even experience tainted presentation [24].

Apart from security concerns based on CIA, there are still many more other concerns like privacy, data segregation, data storage, reliability, security, and data leakage. But out of all, security is the major one where most of the researchers work in the direction to secure cloud more day by day. To ensure the best security, generally data transfer from host to server and vice versa happens with encryption algorithms. Let us take a close look at few of the encryption algorithms.

4 Encryption Algorithms Used to Ensure Cloud Security

Earlier when data was stored on-premise, security measures were levied across the institute, as the data used to be always on the traditional server residing in the organization itself. But gradually, when we have started migrating on the cloud, which is global, an essential security check to ensure data integrity, privacy, and availability have become a major concern. To avoid the flaws, strong encryption techniques are being implemented [25]. Below mentioned are kinds of encryption algorithms used to ensure data security on cloud.

- RSA Algorithm:

This is the most commonly known algorithm, named after Rivest, Shamir, and Adleman, the discoverer. It is a kind of asymmetric algorithm where an encryption key is shared publicly to all but for encrypting a message, but the decryption key is kept private and not publically. Moreover, RSA is a block cipher where each message is charted in an integer. When used on the cloud, a cloud service provider does the encryption of data, place the key publically and the user who accesses this data from cloud, will decrypt it through a private key. RSA algorithm is found to be secure only for the users, but doesn't provide scalability and uses more of memory space which is basic problems with RSA [26].

- DES Algorithm:

DES stands for Data Encryption Standard. It is a symmetric block cipher algorithm. In this, data is encrypted in 64 bits of block size. Hence, 64 bits of data is input and encrypted to 64 bits of cipher text. DES also ensures security at both the ends and is scalable also. But it requires more memory space as compared to AES algorithm [27].

- 3DES Algorithm:

3DES utilizes three occurrences of DES with different keys. It is deemed to be secure because it needs operations enumerated to 2^112 to break it and none of the recent technologies make it possible within the harmful duration of time. It is inherently slow in case of of implementations, as it was premeditated to perform on-chip rather than by chip [28]. Block diagram of Triple DES implementation is as shown in Fig. 1 [29].

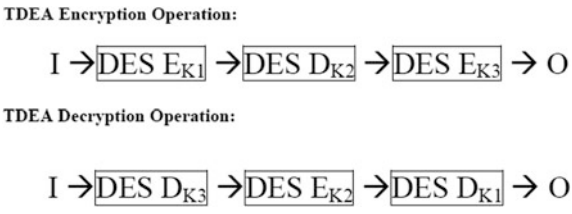

Fig. 1 Block diagram of TDES

- AES Algorithm:

AES stands for Advanced Encryption Standard, and is a symmetric block cipher kind of algorithm, used maximum nowadays. AES follows 128-bit key length for encryption. In this type of algorithm, a data when is about to be stored on cloud by the data generator, it is encrypted first and then this encrypted data is stored on cloud. When any end users would like to use this data, the decryption takes place at the data generator's end and then only the users will be able to read data on their side. AES is found to be highly scalable and is also providing security at both the ends, i.e., users and the providers. Even the memory usage for AES kind of encryption is found very low [30].

- Blowfish Algorithm:

Blowfish is a symmetric key cryptographic algorithm. It encrypts blocks of size 64 bits with a changeable length key of size 128–448 bits. Blowfish is suitable for those applications where the key does not change frequently but remains constant for a very long time. Blowfish is also secured for both the users and the providers, and is also scalable. It is providing with good authenticity but is less used than AES [31].

The encryption algorithms are very essential and provide a better mechanism to secure data on cloud. As data security on cloud is the major concern, and as CIA are very essential for cloud security, a model proposed below, known as RD Model, is designed in such a way that it ensures all three very diligently.

5 Proposed RD Model

An RD Model is proposed with its architecture, depicted in Fig. 2, for communication between client and server, from client side. A similar reverse channel would exist from server to client communication. The model takes the data from the client in respective protocol as chosen by the client, and takes it into the defined encryption stages as below:

Step 1: Encryption Stage 1:

A random or pseudorandom pattern is generated to be used as key for the first time only. Later on, in the next cycles this key can be provided by the other party and may also be used to acknowledge previous communication. It will also check integrity of the complete path.

Step 2: Scrambling of data:

In this step, the key and the data are scrambled together which would generate another set of pseudorandom stream.

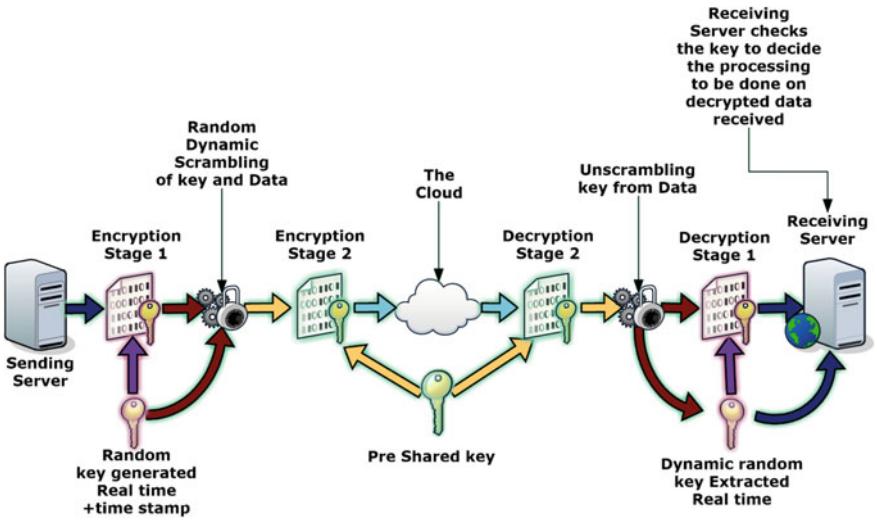

Fig. 2 Proposed RD model

Step 3: Encryption stage 2:

This is the normally used Public-Key Infrastructure (PKI), which uses a symmetric or an asymmetric keying technique as available in the network.

Step 4: Data stream in the cloud:

After the encryption stage 1 of the sender's data, scrambled data with further encryption using PKI will now be transmitted over the cloud.

Step 5: Decryption stage 2:

This stage is the corresponding complementary stage for encryption stage 2 as depicted in step 3.

Step 6: Unscrambling of data and key:

The unscrambling will be in perfect coordination to the pseudorandom scrambling of the data and the key done in step 2. In this stage, the scrambled key is extracted and retrieved accurately.

Step 7: Decryption stage 1:

It contains the exact complementary decryption algorithm as discussed in step 1 and it retrieves the data sent using the key extracted in previous step.

Step 8: Guarantee check on CIA Rules:

Using the key extracted in the step 6, the receiver will check the integrity and authenticity of the received data. This will ensure that only proper data is processed further. If the receiver, based on the preset rules decides that the received data is

objectionable, the data is discarded to avoid further processing. If such a case occurs, a certain set of actions can be levied upon by the receiver which may include a retransmission request or in a worse-case request to login again by session termination.

The security deployed by this algorithm in terms of CIA of the communication far surpasses the disadvantage it suffers from, a comparatively larger overhead in terms of time. The choice of several algorithms in encryption and decryption in the stages and usage of different scrambling mechanisms further ensure the CIA of the communication stream. The process is transparent to the end users making it hard to decipher the algorithm sequence due to the most common security threat, the users themselves. The response sequence can be reutilized as keys for next sequence of data streams as encryption key in Step 1 which also ensures the increased efficiency over a communication and this in turn also works as the logical link between sending and receiving machines to optimize the data flow as well as detection of hidden threats.

6 Conclusion and Future Work

In this paper, an RD model is proposed which uses the first-level encryption followed by scrambling and second-level encryption is carried out. As data security in cloud computing is the most sensitive issue and is seeking utmost attention by researchers, this paper aims at finding a solution for data security implementing second-level encryption and scrambling of data. It also has depicted that the 2-level data decryption ensures data confidentiality integrity and availability at a successful results. The model is designed in MATLAB with implementation of 3DES algorithm at present. It also shows the use of scrambling and unscrambling of data, which ensures integrity and authenticity of transmitted data. In future, this model will be demonstrated on Java platform to implement a real time model, so that data security is guaranteed on cloud computing world without any doubts on the vulnerabilities of cloud.

References

1. Murugesan S (2011) Cloud computing gives emerging markets a lift. IT Pro, IEEE, pp 60–62
2. National Institute of Standards and Technology (2008) Guide for mapping types of information and information systems to security categories. NIST 800-60
3. Hashizume K et al (2013) An analysis of security issues for cloud computing. J Internet Serv Appl 4(1):1–13

4. Zhu W, Luo C, Wang J, Li S (2011) Multimedia cloud computing. IEEE Signal Process Mag 59–69
5. Rimal BP, Choi E, Lumb I (2009) A taxanomy and survey of cloud computing. In: 2009 fifth international joint conference on INC, IMS and IDC, IEEE, pp 44–51
6. Tangwongsan S, Itthisombat V (2014) A highly effective security model for privacy preserving on cloud storage. Cloud Comput Intell Syst (CCIS). In: IEEE 3rd international conference
7. Somani U, Lakhani K, Mundra M (2010) Implementing digital signature with RSA encryption algorithms to enhance the data security of cloud in cloud computing. IEEE
8. Rafique S et al (2015) Web application security vulnerabilities detection approaches: a systematic mapping study. In: 16th IEEE/ACIS international conference on software engineering, artificial intelligence, networking and parallel/distributed computing (SNPD). IEEE
9. Fernandes DAB et al (2014) Security issues in cloud environments: a survey. Int J Inf Secur 13(2):113–170
10. GroBauer B, Walloschek T, Stocker E (2011) Understanding cloud computing vulnerabilities. IEEE, pp 50–57
11. Schneiderman R (2011) For cloud computing, the sky is the limit. IEEE Signal Process Mag 15–17
12. Heier H, Borgman HP, Bahli B (2012) Cloudrise: opportunities and challenges for IT governance at the dawn of cloud computing. In: 45th Hawaii international conference on system science (HICSS). IEEE
13. Gartner (2008) Assessing the security risks of cloud computing. Gartner
14. Parekh DH, Sridaran R (2013) An analysis of security challenges in cloud computing. In: IJACSA
15. Cloud Security Alliance (2010) Top threats to cloud computing, Cloud Security Alliance
16. Harauz J, Kaufman LM, Potter B (2009) Data security in the world of cloud computing, IEEE, pp 61–64
17. Aazam M et al (2014) Cloud of things: integrating internet of things and cloud computing and the issues involved. 2014 11th international Bhurban conference on applied sciences and technology (IBCAST)
18. Yu S, Wang C, Ren K, Lou W (2010) Achieving secure, scalable, and fine-grained data access control in cloud computing
19. Yu S, Ren K, Lou W, Li J (2009) Defending against key abuse attacks in kp-abe enabled broadcast systems, In: Proceedings of SECURECOMM'09
20. Wang C et al (2010) Privacy-preserving public auditing for data storage security in cloud computing. In: Proceedings of INFOCOM. IEEE
21. Wang Q et al (2009) Enabling public verifiability and data dynamics for storage security in cloud computing. In: Computer Security—ESORICS 2009. Springer, Berlin, pp 355–370
22. Armbrust M et al (2010) A view of cloud computing. Commun ACM 53(4):50–58
23. Zhang Q, Cheng L, Boutaba R (2010) Cloud computing: state-of-the-art and research challenges. J Internet Serv Appl 1(1):7–18
24. Popović K (2010) Cloud computing security issues and challenges. In: MIPRO, proceedings of the 33rd international convention. IEEE
25. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Network Comput Appl. Elsevier, pp 1–11
26. Sun D et al (2011) Surveying and analyzing security, privacy and trust issues in cloud computing environments. Proc Eng 15:2852–2856
27. Buyya R et al (2009) Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Fut Gener Comput Syst 25(6):599–616
28. Shao J, He Z (2004) High-speed implementation of 3DES encryption algorithm based on FPGA. Mod Electron Technol
29. National Institute of Standard and Technology (1999) Data encryption standard (DES)[EB/OL]. http://www.csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

30. Sanaei Z et al Heterogeneity in mobile cloud computing: taxonomy and open challenges. Commun Surv Tutorials 16(1):369–392
31. Xiao Z, Xiao Y (2013) Security and privacy in cloud computing. Commun Surv Tutorials 15 (2):843–859

Author Biographies

Prof. Disha H. Parekh, M.Phil., MCA, PGDBA (Human Resource), is presently an Assistant Professor of Faculty of Computer Applications at Marwadi Education Foundation's Group of Institutions, Rajkot, Gujarat. She has completed her M.Phil. in Computer Science from Bharathiar University and is at present pursuing Ph.D. in computer science on cloud computing. She did her MCA from Ganpat University, Gujarat. She even completed PGDBA with a specialization in HR from Symbiosis University. She has published 3 papers in the International Journal and has presented 1 paper at National conference. She has attended many workshops and seminars. Her areas of interest are Software Engineering and Web Technologies.

Dr. R. Sridaran, is currently the Dean, Faculty of Computer Applications, Marwadi Education Foundation's Group of Institutions, Rajkot, Gujarat. He did his postgraduation in Computer Applications and Management. He was awarded Ph.D. in Computer Applications in 2010. Having started his career as an Entrepreneur, he has offered his consultancy services to various service sectors. He designed and delivered various training programs in the areas of IT and Management. He has published 15 research papers in foremost Journals and Conferences and is currently guiding five research scholars. He has got 22 years of academic experience and has served in principal educational institutions at diverse capacities.