Review Article

International Journal of Advanced Computer Research, Vol 6(27)
ISSN (Print): 2249-7277 ISSN (Online): 2277-7970
http://dx.doi.org/10.19101/IJACR.2016.626005

Review of solutions for securing end user data over cloud applications

Akashdeep Bhardwaj[1*], GVB Subramanyam[2], Vinay Avasthi[1] and Hanumat Sastry[1]
College of Engineering Studies, UPES, Dehradun, India[1]
Tech Mahindra, United States of America[2]

Received: 17-June-2016; Revised: 15-September-2016; Accepted: 20-September-2016

Abstract
There is an urgent need of solutions for end user data protection and privacy during the times when migrating from one cloud service provider to another. This paper reviews the challenges in cloud computing services regarding end user data, analyzing the issues and presented solutions to overcome them. The end user data required to be protected in four different ways ranging from usage data which is the information collected from computer systems, the second is the sensitive information on health and bank accounts, third is the personally identifiable information; information to identify an individual and finally is the unique device identity information that is uniquely traceable like IP addresses, unique hardware identities (media access control (MAC) address). By using solution paths such as digital keys, multi factor authentication and cloud aware applications. This paper identifies end users data security issues when using cloud computing services. The focus is directed to critical issues related to unauthorized access for integrity during data in transit. It can be addressed using public key cryptography or public key infrastructure (PKI) for confidentiality and data integrity of end user data over the cloud. Then for migrating from one cloud service provider to another, data security and privacy are addressed by cloud aware applications. Lastly, using multi factor authentication combined with network and application detection systems, intrusion detection systems and network traffic routing in case of cyber-attacks, can help in denial of service attack mitigation or prevent man in the middle and network snooping attacks in cloud computing.

Keywords
Cloud security, Cloud computing, Public key cryptography, PKI.

1. Introduction
Cloud based services provide flexible, scalable, pay-per-use, a short term contract model for the IT services. Cloud based services are an efficient, affordable and easy to implement option, reducing capital expenditure involving IT hardware, licenses, office space, computing power and bandwidth. Cloud security of user data needs to be more emphasis as it is being hosted on the service provider premise as well as the end user residing in a remote data center. So it is outside the user's control. When there is a need to provide authentic IT resources to the end users to enable them to perform their tasks, usually we do not emphasize on the importance of securing the end user data. End user data for end user functionalities such as support, buying hardware, software and licenses, then plan endlessly for installation, support, maintenance as well as worry about capacity planning, creating intrusion detection system (IDs), configuring profiles or sit on a budgeted pile of money waiting for hiring to be completed [1].

*Author for correspondence

Web based services: Internet email services (Gmail, Yahoo, and Hotmail), Online stores (Amazon, Fab furnish, Jabong) and Web hosting (NetMagic, Tulip). These have been around for many years.

Distributed computing: Splitting the processing workload among multiple systems usually connected at the same sites like being done in parallel and grid computing technologies.

Datacenters: Single application being hosted in one location (over single or even multiple servers) does not qualify as a Cloud. Cloud computing leverages pooled hardware resources, automation services involving a great deal of virtualization hosted across data centers. On these avenues, there are different types of security challenges and versatile solutions for each of the cloud deployment models and also overcome them as well [2].

The important cloud service models are as follows:

- Software as a service (SaaS) is on demand model where users accessing the applications over the cloud. Some of the examples are an on-demand

CRM Salesforce, Google Apps, Microsoft Office 365 and Microsoft Sky Drive.

- Platform as a Service (PaaS) provides end users with complete environment so that developers can deploy their apps, perform testing and hosting of web applications and databases with the help of virtual servers. Examples are Google apps, Azure from Microsoft and Rackspace.
- Infrastructure as a Service (IaaS) provides hardware and computing power to end user to provision and harness resources from computing, network devices, storage or servers where the customers pay only for the amount of infrastructure used and not worry about buying hardware, maintaining or upgrading issues [3]. Infrastructure can be scaled up or down dynamically based on application resource and market demands. Some of the examples are Amazon elastic compute cloud (EC2), Rack Space, Attenda RTI, Eucalyptus (Open source).

2. Challenges in cloud computing

2.1End user challenges in the cloud

End users typically face the following challenges in cloud computing:

- Limited support for customization: there are limits to the amount of customization that can be done for cloud applications and services to suit end user specific requirements.
- Constraints on features: cloud apps tend to be less feature rich as compared to their on-site or in-house counterparts because of inbuilt capabilities.
- Application latency: latency becomes a major factor for Cloud apps that are dependent on the transfer of large volumes or time sensitive data [4].
- Statelessness: performance issues arise for Cloud apps as the communication is unidirectional, single requests and responses from end users traveling to and from a service provider experience drop or disconnects travel over different paths/routes tend to arrive out of sequence.
- Legal restrictions: at times force organizations to secure and control its data in a specific geographical location for the cloud provider's data center.
- Security of end user data is the most critical issue, depends on the cloud provider's architecture and model, cloud vendors, is primarily responsible for managing environmental and virtualization security, ensuring security, authentication, integrity and privacy of data stored on their sites or in transit over unsecure internet links. Here data breaches, compromised credentials/broken authentication, hacker interfaces and APIs, system vulnerabilities due to zero day attacks, account hijacking, malicious insider threats, advanced persistence threats, permanent data loss, inadequate compliance checks, distributed denial of service (DDoS) attacks and use of shared resources and storage are among the most critical security issues plaguing end users and their data.

Typical concerns raised by end users to cloud service providers (CSPs) when adopting cloud services are

- How cloud services providers instill confidentiality and integrity of end user data?
- How should the CSPs protect stored data from attacks which is in their cloud data centers?
- How to change CSPs and be able to move and migrate from one CSP to another?

2.2Gaps around end user computing applications

While the confidentiality, integrity and availability triad is the most critical in development, maintenance and availability of cloud application during regular execution for any business enterprise, check on unauthorized users using organization email or sharing critical end user documents or financial data is essential to be performed on a regular basis. Another critical gap could be the application data stored in business users' computers-this leads to confidentiality issues. Absence of any strong and appropriate access control may allow end users or other potential violators can alter the integrity of end user computing applications leading to take an improper business decision. Many a times, the end user computing configuration items typically reside and stored on the user local system or in shared drives, not following the right change management processes. Also lack of access control leads to accidental and intentional manipulation of the end user data or their application configuration items which ends up causing availability and integrity issues. Risk assessment controlling areas can be defined which need to include input/ output/edits, data processing, report / output file, backups, business continuity plans, change management, incident / problem management, access provisioning, data privacy, monitoring, disposal of end user computing application and disposal of end user data.

3. Literature review

Modern information threat vectors for end user data have risen in the recent years, these ranges from hackers on hire seeking to steal end user intellectual property data to employees unaware about data security and protection. Proper data protection systems need to be in place and a culture of security

awareness needs to be a high priority goal of the information security team. European network and information security agency (ENISA) have identified thirty five security risks, further subdividing them into policy, organizational risks, legal risks, technical risks and non-cloud related. From these risks, the ENISA identified eight most important risks, five of which directly or indirectly relate to data confidentiality risks. These risks include isolation failure, malicious insider threats, data protection, insecure data deletion and management interface compromise. Similarly, cloud security alliance (CSA) identifies the thirteen kind of risks related to the cloud computing. From among the thirteen risks, CSA declares seven high priority risks, five of which are directly or indirectly involved with data confidentiality which includes: malicious insiders, insecure application programming interfaces, traffic hijacking and account service and data losses.

In 2015, Gholami et al. [5] suggested a new cloud security model related to quality of service(QoS) for end user data regarding confidentiality of the outsources data on the cloud in the form of a neural data security model. This ensured security and high confidentiality using RSA security algorithm.

In 2013, Hu et al. [6] addresses data security access control model for secure data access based on MAC control for government cloud platform model. This model includes necessary technical strategies to ensure data security during access. They reviewed relationships between risk factors and expected solutions. Data access security model with a 3-stage control technology had been proposed with high reliability for data displayed.

A review of data security issues in a cloud computing environment presented in a unique cloud computing pattern with resources being provided on demand via internet [7]. Security and privacy issues related to cloud and its data storage are analyzed in the paper along with various attacks on cloud computing. Challenges like security issues, data challenges were identified along with solutions regarding the security issues.

In 2014, Hemalatha et al. [8] addresses a comparative analysis of encryption techniques and data security issues in cloud computing. Cloud computing technologies regarding two delivery models, cloud classification and encryption mechanisms was discussed. A comparative study was made based on the encryption techniques to maintain the security and confidentiality over a cloud. They classified in various parts regards to data storage, integrity, backup and recovery, security and confidentiality. The importance of data privacy and security is analyzed and encryption techniques used in cloud environment are compared.

In 2012, Xin et al. [9] addresses research on cloud computing, data security model based on multi dimensions. A complete data security three layer defence model based on multi dimension is proposed. User authentication and unauthorized user access are discussed. Every layer has their own role yet combine with each other to data security in cloud computing environments.

In 2012, Wang et al. [10] presented a hybrid cloud computing model based on data security and authentication. Various methods to protect user data was discussed in regards to security which includes single encryption, multilevel virtualization and authentication interface based on PKI and certificate authority (CA) model for better performance.

In 2014, Moghaddam et al. [11] proposed an efficient, scalable user authentication model scheme for cloud computing environments by designing user authentication and access control model to enhance the rate of trust and reliability. Separate server systems with stores authentication and cryptography resources from the real time servers was proposed, these help decrease the user authentication dependency and the encryption process on the main authentication server.

4. Proposed solutions for resolving cloud data security issues

4.1 End user security using public key cryptography

For authentication and integrity issues public key cryptography implementation seems to be the right approach. It is shown in the *Figure 1*. When data are in transit over unsecure internet circuits, unauthorized access of end user data is the main security issue faced by cloud computing services. To resolve the cloud service provider's security issue of authentication and integrity, public key cryptography should be used, for the encryption and decryption of digital data. Encryption is the conversion of data into seemingly random, incomprehensible data which ensures that data remains jumbled to everyone for whom it is not intended, even if the intended user has access to the encrypted data.

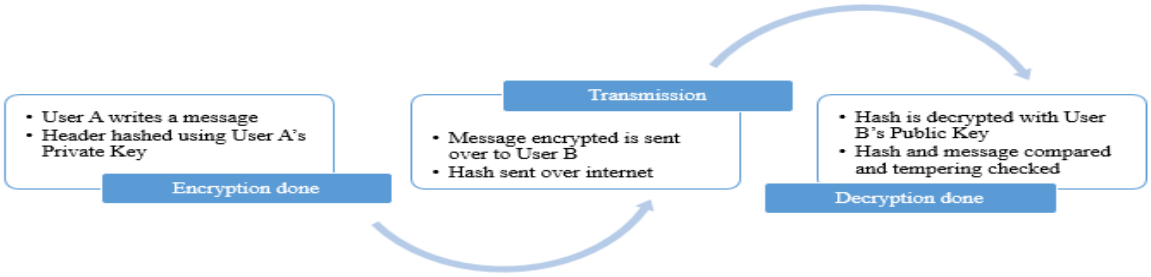

Figure 1 Encryption-decryption process

Using the PKI framework which internally has security policies, communication protocols, and procedures to enable secure and trusted communication between CSPs and the end users over unsecure internet circuits and cloud computing environments inside as well as outside the organization [12]. The public key infrastructure is on the hybrid mode encryptions like symmetric and asymmetric. The only option for transforming the user data back into intelligible form is to reverse the encryption or decryption using single secret key or two secret keys (public and private). The public key is available to everyone via a public repository or directory while the private key remains confidential to its respective owner [13]. Since the key pairs are related mathematically, whatever is encrypted with a public key may only be decrypted by its corresponding private key and vice versa. Public key crypto is enabled in the cloud by means of:

- Each entity encrypts data using their own private keys.
- All systems and elements in the system such as cloud computing infrastructure units, platform, virtualization tools and other involved entities have their own keys.
- While fulfilling their own functions of information exchange and processing, all the systems and elements will use the public key and private key to perform authentication first.
- Events that occur in the cloud computing have also assigned a unique key.
- In this way, crypto cloud system guarantees the security and credibility of information exchange.
- To reap the advantages of cloud computing, service providers are best advised to go to the following practices and design features of PKI that can further enhance the security.
- Key management server (KMS) should be implemented inside the organization, for the enterprise data stored in the cloud requires encryption keys to decrypt as an end-user request, which only the key management server provides them [14]. The encryption keys for decrypting data from cipher text to the original plain text should not be on the cloud virtual machines, and security process is implemented so that these keys should reside in-memory for a few seconds.
- Any data moving out or coming in of the data centers can be encrypted and decrypted respectively.
- The virtual machines hosted in the Cloud provider's environment should be encrypted at all point of times in order to protect any kind of data loss in case the virtual snapshot is compromised.
- In case data encryption is not required, the service provider should revoke any keys associated so that even any sort of data trail remains in the system, it cannot be decrypted.
- Storage of keys should be done using the hardware security model (HSM) for performing encryption and decryption.
- Unsecure encryption algorithms such as RC4, MD5, SHA-1 and data encryption standard (DES) must always be avoided.
- Advance encryption standard (AES) is the symmetric key block cipher algorithm to provide cloud data security. This block cipher uses 128 bit block size and key length can be 128, 192, and 256. Advantages of AES:
  - Performs in software and hardware platform environments with equal ease.
  - Inherent process facilities resulting in very good software performance.
  - Speedy key setup time and good key ability.
  - Less memory for implementation.
  - Benefits from instruction level parallelism.
  - No serious weak keys in AES.

4.2Use multi factor authentication

Multifactor authentication or use of at least two separate identifiers of authentication instead, using just an Id and password helps increase security access by adding multiple barriers to inbound user access before actual entry is allowed. In doing so, this reduces the likelihood of an attacker break in place at the same time makes it harder for anyone with a

stolen password to gain entry to the system accessing critical data. To protect the user data stored in cloud servers from external attacks using multi factor authentication, firewalls, and load balancers with specific ports and IDS intrusion detection system [15]. Establishing robust data center architecture and protection system process for cloud storage systems by applying the following:

- Multi factor authentication (MFA): it is the user knows (password) and something the user has been provided by the cloud provider (RSA Token). It is shown in the *Figure 2*.
- Security systems like firewalls and load balancers before the storage servers which allow only specific ports and data flow inside the cloud data centers.
- IDS to detect unauthorized activities in four main areas-
  - In the virtual machine (VM) itself: by deploying IDS on the VM, IDS can monitor the system activity to detect and alert on issues that may arise.
  - In the hypervisor or host system: by having the IDS deployed on the hypervisor host, IDS can monitor the hypervisor as well as traffic between VMs running on the hypervisor. It is a more centralized location for IDS, but there may be issues in keeping up with performance or dropping some information in case the amount of data is huge.
  - In the virtual network: by deploying the IDS within the host, the virtual network monitoring can be done, which allows the IDS to monitor the network traffic between the virtual machines on host systems, as well as the traffic between the host and VMs [15]. This "network" traffic never hits the traditional network.
  - In the traditional network: Deploying IDS allows IDS to detect and alert regarding the traffic passes from the network devices and infrastructure.
  - Using different virtual local area networks (VLANs) and Switches inside data centers for inbound and outbound traffic using.
  - Limiting user access and separation of data is done by applying separation of the data that is being stored in servers as per end user profiles, i.e. read-only for external level 1 user, read-write for corporate employee as level 2, read-write-delete-modify for enterprise administrators as level 3 users.

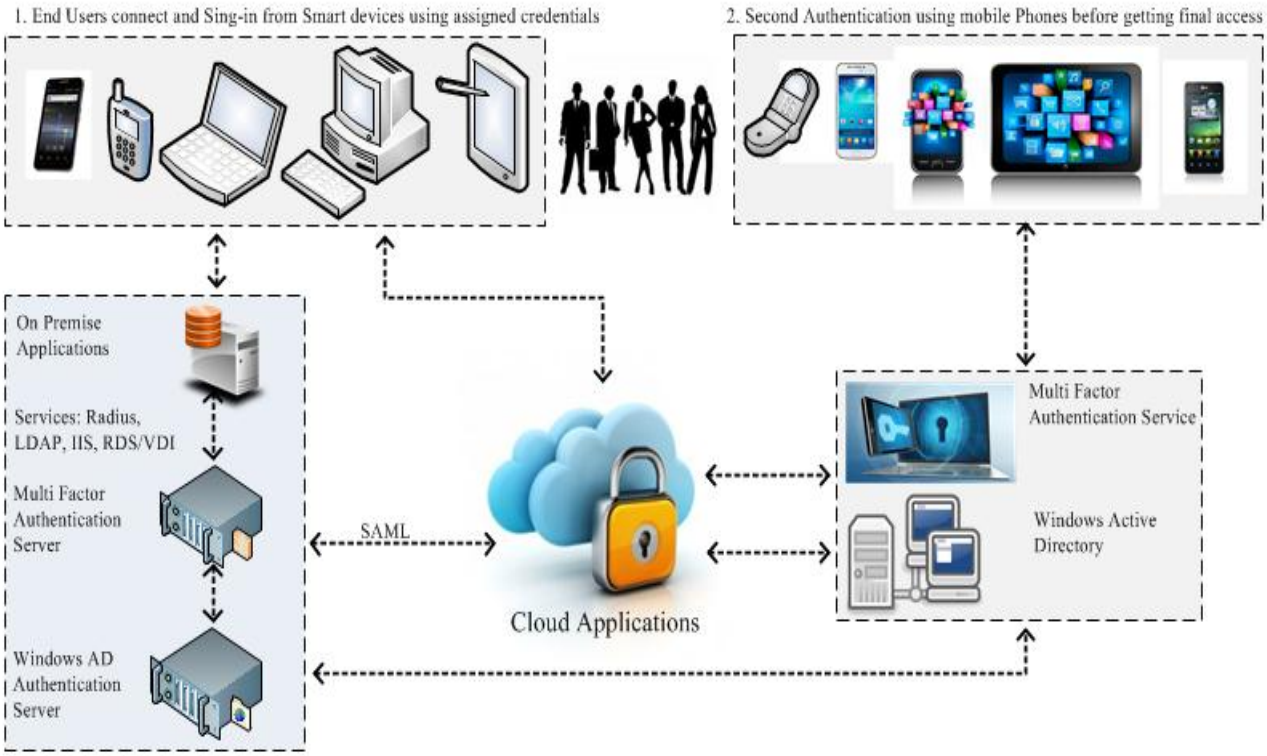

Figure 2 Multi factor authentication overview

Real time examples of multi factor authentication use are Office 365 and Azure MFC. Within Office 365 Exchange, Sharepoint, Lync, Dynamics CRM, Project Management and Office 2013 can be used in multi factor authentication.

4.3Use of cloud aware applications

Provisioning users migrating from one cloud provider to another and move their applications, data and services between cloud providers by ensuring implementation of cloud aware architectures. It ensures the applications being built are cloud-aware [16] and cloud migration planning which is performed in the new cloud provider's data center. Application need to be made more cloud-aware for which there is a need to:

- Review code and then architect applications to increase cloud portability.
- Design and develop open standards for cloud computing.
- Use tools that can work to move applications around clouds without any modifications.

For the cloud migration planning there is a need to involve the following-

- Discovery of new environment.
- Application, server and data migration plan.
- Post-migration, configuration.
- Verification testing.

During the migration from one cloud service provider to another, users should also include checking on the use of standardized storage protocols, for example the ISO standard cloud data management interface (CDMI) by providers for the integration and trust relationship with other providers [17]. Cloud aware applications have the ability to decrease server count and are able to handle the massive workload by virtue of the ability to scale elastically, maximize tenants and minimize idle computing resource. Furthermore to reduce data transfer costs application developers and data center handlers need to:

- Minimize payload sizes by using APIs that return only the data required by the consumer needs and perform data compression, reduce CPU computing cost of encoding and decoding.
- Minimize data transfers by using cache immutable data and seek to replace "chatty" protocols.
- Instrument code by tracking data transfers throughout an application, which helps identify optimization options and the use of load traffic generation tools which can provide insight into the impact of such optimizations.

Cloud aware application maturity model provides a simple way to assess the level of cloud maturity of an application, just as the Richardson maturity model measures the maturity of an API [18]. The maturity model suggests changes that can be implemented to increase an application's resilience, flexibility, and scalability in a cloud environment. As listed in *Table 1* below, there are four levels to the maturity model with level 3 representing the highest level of maturity and level 0 representing applications that are not cloud aware.

Table 1 Cloud aware application maturity levels

Maturity level	Application description
Level 3: Adaptive	Dynamically migrate infrastructure between providers without any service.
	The application can dynamically scale out or scale in based on stimuli.
Level 2: Abstracted	Services are stateless.
	The application is unaware, unaffected by dependent service failures.
	The application is infrastructure agnostic and can run anywhere.
Level 1: Loosely Coupled	The application is composed of loosely coupled services.
	The application services are discoverable by name.
	The application computes and storage are kept separated.
	The application consumers one or more cloud services: compute, storage, and network.
Level 0: Loosely Coupled	The application runs on virtualized infrastructure.
	The application can be instantiated from an image or script.

5. Research work performed

The authors' setup web application server using .NET framework 2.0 with the Windows 2012 standard edition running IIS using HTTPS and SQL Server 2008 as the backend for admin portal to set up the multi factor authentication system as a system for user access to the cloud service and created a one-time-password (OTP) client application. The authentication process is defined as follows and described in the *Figure 3* below.

- User registered and verified end user mobile for receiving SMS.
- SMS received by the mobile is actually a 4 digit verification code in the form of OTP.

- To register and verify OTP device, and pair with a cloud account, the OTP client application scan and verify the code form.
- Once done a passcode is generated to enter on the cloud site along with the end user name and password as shown in the *Figure 4*.

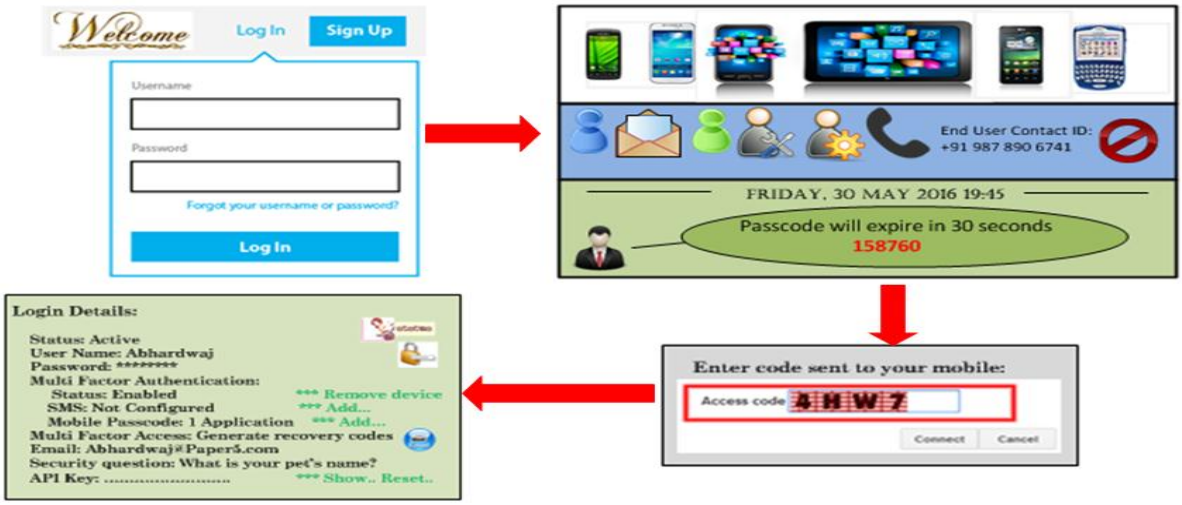

Figure 3 Web applications with OTP authentication

Figure 4 Traffic flow for end user authentication

6. Conclusion

In this paper the authors identified issues that end users face when using cloud computing services. Three specific issues and solutions for making data on the cloud more secure from unauthorized access for integrity during transmission with the public key cryptography have been suggested. Security systems and solutions are used to enable end users to have their data interoperate with different cloud providers when migrating from one cloud provider to another. The result analyses are as follows:

- Public key cryptography can help in achieving confidentiality and data integrity of end user data over the cloud.
- With cloud-aware apps, proper cloud migration planning and use of standard cloud storage protocols between the cloud provider helps in achieving application and data migration between providers in a smooth manner.
- Using multi factor authentication along with intrusion detection systems and network traffic routing helps in achieving mitigation from attackers for cloud computing.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Schutz C, Gao Y, Hou D, Powers S, Grimberg S, DeWaters J. A time series data transformation engine for non-programmer end users. In 3rd MEC international conference on big data and smart city (ICBDSC) 2016 (pp. 1-7). IEEE.

[2] Bouchana S, Idrissi MA. Towards an assessment model of end user satisfaction and data quality in business intelligence systems. In 10th international conference on intelligent systems: theories and applications (SITA) 2015 (pp. 1-6). IEEE.

[3] Salvi S, Sanjay HA, Rangavittala SR. An encryption, compression and key (ECK) management based data security framework for infrastructure as a service in cloud. In IEEE international advance computing conference (IACC) 2015 (pp. 872-6). IEEE.

[4] Fallon L, OSullivan D. SECCO: a test framework for controlling and monitoring end user service sessions.

In IEEE network operations and management symposium (NOMS) 2014 (pp. 1-7). IEEE.
[5] Gholami A, Arani MG. A trust model based on quality of service in cloud computing environment. International Journal of Database Theory and Application. 2015; 8(5):161-70.
[6] Hu J, Chen L, Wang Y, Chen SH. Data security access control model of cloud computing. In international conference on computer sciences and applications (CSA) 2013 (pp. 29-34). IEEE.
[7] Zatakiya S, Tank P. A review of data security issues in cloud environment. International Journal of Computer Applications. 2013; 82(17):15-8.
[8] Hemalatha N, Jenis A, Donald AC, Arockiam L. A comparative analysis of encryption techniques and data security issues in cloud computing. International Journal of Computer Applications. 2014; 96(16):1-6.
[9] Xin Z, Song-qing L, Nai-wen L. Research on cloud computing data security model based on multi-dimension. In international symposium on information technology in medicine and education (ITME) 2012 (pp. 897-900). IEEE.
[10] Wang JK, Jia X. Data security and authentication in hybrid cloud computing model. In IEEE global high tech congress on electronics (GHTCE) 2012 (pp. 117-20). IEEE.
[11] Moghaddam FF, Moghaddam SG, Rouzbeh S, Araghi SK, Alibeigi NM, Varnosfaderani SD. A scalable and efficient user authentication scheme for cloud computing environments. In IEEE region 10 symposium 2014 (pp. 508-13). IEEE.
[12] Hang F, Zhao L. Supporting end-user service composition: a systematic review of current activities and tools. In IEEE international conference on web services (ICWS) 2015 (pp. 479-86). IEEE.
[13] Fidas C, Sintoris C, Yiannoutsou N, Avouris N. A survey on tools for end user authoring of mobile applications for cultural heritage. In 6th international conference on information, intelligence, systems and applications (IISA) 2015 (pp. 1-5). IEEE.
[14] Tzeremes V, Gomaa H. XANA: an end user software product line framework for smart spaces. In 49th Hawaii international conference on system sciences (HICSS) 2016 (pp. 5831-40). IEEE.
[15] Hylli O, Lahtinen S, Ruokonen A, Systä K. Resource description for end-user driven service compositions. In IEEE world congress on services 2014 (pp. 11-7). IEEE.
[16] Yao X, Han X, Du X. A light-weight certificate-less public key cryptography scheme based on ECC. In 23rd International conference on computer communication and networks (ICCCN) 2014 (pp. 1-8). IEEE.
[17] Vollala S, Varadhan VV, Geetha K, Ramasubramanian N. Efficient modular multiplication algorithms for public key cryptography. In IEEE International advance computing conference (IACC) 2014 (pp. 74-8). IEEE.
[18] Han X, Wang B, Wang A, Wu L, Rhee W. Algorithm-based countermeasures against power analysis attacks for public-key cryptography SM2. In tenth international conference on computational intelligence and security (CIS) 2014 (pp. 435-9). IEEE.

Akashdeep Bhardwaj PhD research scholar from UPES, PGDM, B.E (Computer Science) is an enterprise risk and resilience technology manager in information security and infrastructure operations having worked with MNCs for over 20 years and he is a certified in Ethical Hacking, Cloud, Microsoft, Cisco, and VMware technologies.
Email: bhrdwh@yahoo.com

Dr. GVB Subrahmanyam PhD is an enterprise architect and focuses on development, delivery and sustenance of IT Applications in supply chain/ insurance/banking/finance. He is a TOGAF certified enterprise architect and IBM certified rational software architect.

Dr. Hanumat G Sastry has received his M. Tech (CSE) from Acharya Nagarjuna University and PhD in computer science from Dravidian University. He has 11 research papers in referred international journals. He has 8+ years of teaching experience at University level. His active research interests include Optimization algorithms, Data mining, Evolutionary computing and Semantic web.

Dr. Vinay Avasthi has received PhD in Computer Science from University of Petroleum & Energy Studies. He has published many Papers at both National and International levels. He has rich experience in Academic & Research includes Data mining, Networking algorithm, distributed computing, cloud computing and IOT. He is the member of ACM, CSI and ISTE. He is also the recipient of CSI Significant Contribution Award 2012-13.