Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Cloud Computing Security Issues

Ch. Deepika[1], P. Swetha[2], Ch. Sreedhar[3]
[1, 2] Assistant Professor,CSE Department, Vidya Jyothi Institute of Technology, C.B.Post.Aziz Nagar, Telangana, India
[3] Assistant Professor, ECE, Nishitha College Engineering & Technology, Telangana, India

Abstract: Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. A new model targeting at improving features of an existing model must not risk or threaten other important features of the current model. The architecture of cloud poses such a threat to the security of the existing technologies when deployed in a cloud environment. Cloud service users need to be vigilant in understanding the risks of data breaches in this new environment. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, enterprise customers are still reluctant to deploy their business in the cloud. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. The advent of an advanced model should not negotiate with the required functionalities and capabilities present in the current model.In this paper, a survey of the different security risks that pose a threat to the cloud is presented. This paper is a survey more specific to the different security issues that has emanated due to the nature of the service delivery models of a cloud computing system.

Index Terms—Cloud computing Data privacy Data protection Security Virtualization

I. INTRODUCTION

Today Small and Medium Business (SMB) companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best business applications or drastically boost their infrastructure resources, all at negligible cost.. Cloud providers currently enjoy a profound opportunity in the marketplace. The providers must ensure that they get the security aspects right, for they are the ones who will shoulder the responsibility if things go wrong. The cloud offers several benefits like fast deployment, pay-for- use, lower costs, scalability, rapid provisioning, rapid elasticity, ubiquitous network access, greater resiliency, hypervisor protection against network attacks, low-cost disaster recovery and data storage solutions, on-demand security controls, real time detection of system Gartner (Jay Heiser, 2009) defines cloud computing (Stanojevi et al., 2008; Vaquero et al., 2009; Weiss, 2007; Whyman, 2008; Boss et al., 2009) as ''a style of computing where massively scalable IT- enabled capabilities are delivered 'as a service' to external customers using Internet technologies''

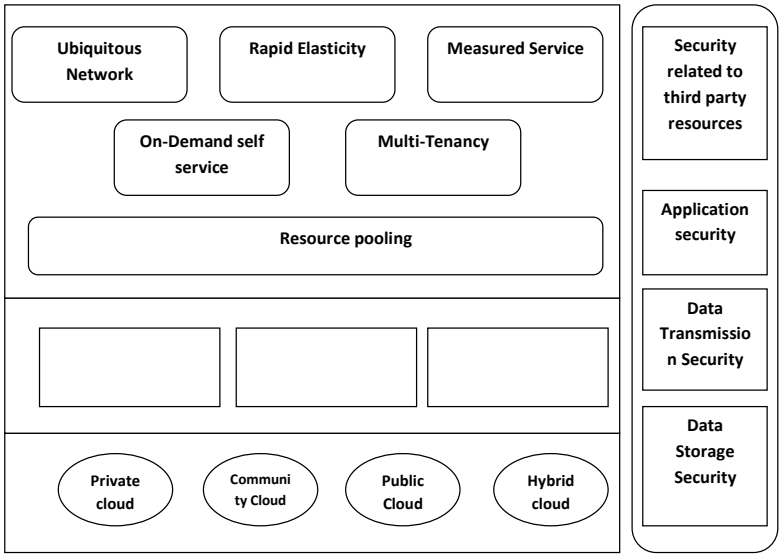

Fig. 1. Complexity of security in cloud environment.

Tampering and rapid re-constitution of services. While the cloud offers these advantages, until some of the risks are better understood, many of the major players will be tempted to hold back (Viega, 2009). According to a recent IDCI survey, 74% of IT executives and CIO's cited security as the top challenge preventing their adoption of the cloud services model (Clavister, 2009). Analysts' estimate that within the next five years, the global market for cloud computing will grow to $95 billion and that 12% of the worldwide software market will move to the cloud in that period. To realize this tremendous

potential, business must address the privacy questions raised by this new computing model (BNA, 2009). These challenges include but not limited to accessibility vulnerabilities, virtualization vulnerabilities, web application vulnerabilities such as SQL (Structured Query Language) injection and cross-site scripting, physical access issues, privacy and control issues arising from third parties having physical control of data, issues related to identity and credential management, issues related to data verification, tampering, integrity, confidentiality, data loss and theft, issues related to authentication of the respondent device or devices and IP spoofing.

II. SECURITY ISSUES IN SERVICE MODELS

Cloud computing utilizes three delivery models by which different types of services are delivered to the end user. The three delivery models are the SaaS, PaaS and IaaS which provide infrastructure resources, application platform and software as services to the consumer. These service models also place a different level of security requirement in the cloud environment. IaaS is the foundation of all cloud services, with PaaS built upon it and SaaS in turn built upon it. Just as capabilities are inherited, so are the information security issues and risks. There are significant trade-offs to each model in the terms of integrated features, complexity vs. extensibility and security. If the cloud service provider takes care of only the security at the lower part of the security architecture, the consumers become more responsible for implementing and managing the security capabilities. A recent survey by Cloud Security Alliance (CSA) & IEEE indicates that enterprises across sectors are eager to adopt cloud computing but that security are needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers. It also details that cloud computing is shaping the future of IT but the absence of a compliance environment is having dramatic impact on cloud computing's growth. Organizations using cloud computing as a service infrastructure, critically like to examine the security and confidentiality issues for their business critical insensitive applications. Yet, guaranteeing the security of corpo- rate data in the ''cloud'' is difficult, if not impossible, as they provide different services like SaaS, PaaS, and IaaS. Each service has its own security issues (Kandukuri et al., 2009).

SaaS is a software deployment model where applications are remotely hosted by the application or service provider and made available to customers on demand, over the Internet.

IaaS completely changes the way developers deploy their applications. Instead of spending big with their own data centers or managed hosting companies or co location services and then hiring operations staff to get it going, they can just go to Amazon Web Services or one of the other IaaS providers, get a virtual server running in minutes and pay only for the resources they use. With cloud brokers like Rightscale, enStratus, etc., they could easily grow big without worrying about things like scaling and additional security. In short, IaaS and other associated services have enabled startups and other businesses focus on their core competencies without worrying much about the provisioning and management of infrastructure. IaaS completely abstracted the hardware beneath it and allowed users to consume infrastructure as a service without bothering anything about the underlying complexities. The cloud has a compelling value proposition in terms of cost, but ''out of the box'' IaaS only provides basic security (perimeter firewall, load balancing, etc.) and applications moving into the cloud will need higher levels of security provided at the host.

PaaS is one layer above IaaS on the stack and abstracts away everything up to OS, middleware, etc. This offers an integrated set of developer environment that a developer can tap to build their applications without having any clue about what is going on underneath the service. It offers developers a service that provides a complete software development lifecycle management, from planning to design to building applications to deployment to testing to maintenance. Everything else is abstracted away from the ''view'' of the developers. The dark side of PaaS is that, these advantages itself can be helpful for a hacker to leverage the PaaS cloud infrastructure for malware command and control and go behind IaaS applications.

III. SECURITY ISSUES IN SAAS

In SaaS, the client has to depend on the provider for proper security measures. The provider must do the work to keep multiple users' from seeing each other's data. So it becomes difficult to the user to ensure that right security measures are in place and also difficult to get assurance that the application will be available when needed (Choudhary, 2007). With SaaS, the cloud customer will by definition be substituting new software applications for old ones. Therefore, the focus is not upon portability of applications, but on preserving or enhancing the security functionality provided by the legacy application and achieving a successful data migration (Seccombe et al., 2009). The SaaS software vendor may host the application on its own private server farm or deploy it on a cloud computing infra- structure service provided by a third-party provider (e.g. Amazon Google, etc.). The use of cloud computing coupled with the pay- as-you-go (grow) approach helps the application service provider reduce the investment in infrastructure services and enables it to concentrate on providing better services to customers. Over the past decade, computers have become widespread within enterprises, while IT services and computing has become a commodity. Enterprises today view data and business processes (transactions, records, pricing information, etc.) themselves as strategic and guard them with access control and compliance policies. However, in the SaaS model, enterprise data is stored at the SaaS provider's data

center, along with the data of other enterprises. Moreover, if the SaaS provider is leveraging a public cloud computing service, the enterprise data might be stored along with the data of other unrelated SaaS applications.The layered stack for a typical SaaS vendor and critical aspects that must be covered across layers in order to ensure security of the enterprise data is illustrated in Fig. 2.

The following key security elements should be carefully considered as an integral part of the SaaS application development and deployment process:

- Data security
- Network security
- Data locality
- Data integrity
- Data segregation
- Data access
- Authentication and authorization
- Data confidentiality
- Web application security
- Data breaches
- Virtualization vulnerability
- Availability
- Backup
- Identity management and sign-on process.

The different security issues of SaaS are discussed as follows.

3.1. Data security:

In a traditional on-premise application deployment model, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. However, in the SaaS model, the enterprise data is stored outside the enterprise boundary, at the SaaS vendor end. Consequently, the SaaS vendor must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data. In cloud vendors such as Amazon, the Elastic Compute Cloud (EC2) administrators do not have access to customer instances and cannot log into the Guest OS.

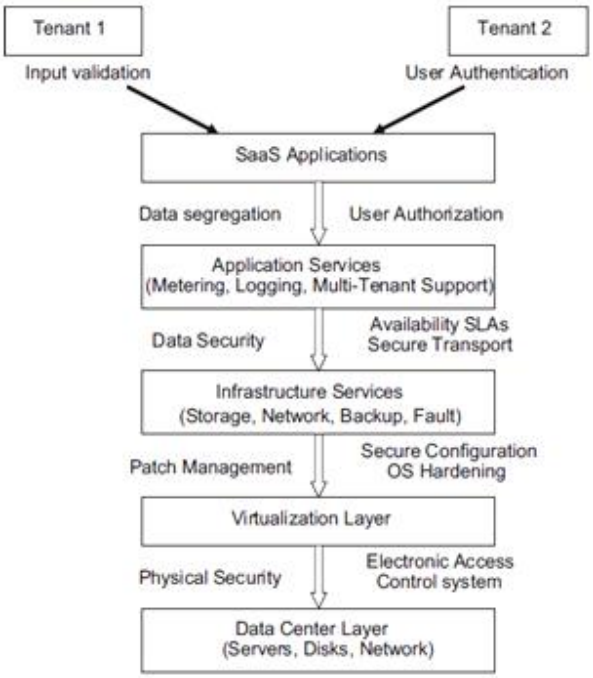

Fig. 2. Security for the SaaS stack.

EC2 Administrators with a business need are required to use their individual cryptographically strong Secure Shell (SSH) keys to gain access to a host. All such accesses are logged and routinely audited. While the data at rest in Simple Storage Service (S3) is not encrypted by default, users can encrypt their data before it is uploaded to Amazon S3, so that it is not accessed or tampered with by any unauthorized party Malicious users can exploit weaknesses in the data security model to gain unauthorized access to data. The following assessments test and validate the security of the enterprise data stored at the SaaS vendor:

- Cross-site scripting[XSS]
- Access control weaknesses
- OS and SQL injection flaws
- Cross-site request forgery[CSRF]
- Cookie manipulation
- Hidden field manipulation
- Insecure storage
- Insecure configuration.

Any vulnerability detected during these tests can be exploited to gain access to sensitive enterprise data and lead to a financial loss.

3.2. Network security:

In a SaaS deployment model, sensitive data is obtained from the enterprises, processed by the SaaS application and stored at the SaaS vendor end. All data flow over the network needs to be secured in order to prevent leakage of sensitive information. This involves the use of strong network traffic encryption techniques such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) for security. In case of Amazon WebServices (AWS), the network layer provides significant protection against traditional network security issues, such as MITM (Man-In-The-Middle) attacks, IP spoofing, port scanning, packet sniffing, etc. For maximum security, Amazon S3 is accessible via SSL encrypted endpoints. The encrypted endpoints are accessible from both the Internet and from within Amazon EC2, ensuring that data is transferred securely both within AWS and to and from sources outside of AWS. However, malicious users can exploit weaknesses in network security configuration to sniff network packets. The following assessments test and validate the network security of the SaaS vendor:

- Network penetration and packet analysis
- Session management weaknesses
- Insecure SSL trust configuration.

Any vulnerability detected during these tests can be exploited to hijack active sessions, gain access to user credentials and sensitive data.

3.3. Data locality:

In a SaaS model of a cloud environment, the consumers use the applications provided by the SaaS and process their business data. But in this scenario, the customer does not know where the data is getting stored. In many a cases, this can be an issue. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in many enterprise architecture (Softlayer, 2009). For example, in many EU and South America countries, certain types of data cannot leave the country because of potentially sensitive information. In addition to the issue of local laws, there's also the question of whose jurisdiction the data falls under, when an investigation occurs. A secure SaaS model must be capable of providing reliability to the customer on the location of the data of the consumer.

3.4. Data integrity:

Data integrity is one of the most critical elements in any system. Data integrity is easily achieved in a standalone system with a single database. Data integrity in such a system is maintained via database constraints and transactions. Transactions should follow ACID (atomicity, consistency, isolation and durability) properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity. Next in the complexity chain are distributed systems. In a distributed system, there are multiple databases and multiple applications. In order to maintain data integrity in a distributed system, transactions across multiple data sources need to be handled correctly in a fail safe manner. This can be done using a central global transaction manger. Each application in the distributed system should be able to participate in the global transaction via a resource manager. This can be achieved using a 2-phase commit protocol as per XA standard. Enter the world of SOA and Cloud computing, and the problem of the data integrity gets magnified even more, as there is a mix of on-premise and SaaS applications exposed as service. SaaS applications are multi-tenant applications hosted by a third party. SaaS applications usually expose their functionality via XML based APIs (Application Program Interfaces). Also, in SOA based environments, many on-premise applications expose their functionality via SOAP and REST web services as well. One of the biggest challenges with web services is transaction management. At the protocol level, HTTP (Hyper Text Transfer Protocol) does not support transactions or guaranteed delivery, so the only option is to implement these at the API level. Although there are standards available for managing data integrity with web services such as WS-Transaction and WS-Reliability, these standards are not yet mature and not many vendors have implemented these. Most SaaS vendors expose their web services APIs without any support for transactions. Also, each SaaS application may have different levels of availability and SLA (service-level agreement), which further complicates management of transactions and data integrity across multiple SaaS applications. The lack of integrity controls at the data level (or, in the case of existing integrity controls, bypassing the application logic to access the database directly) could result in profound problems. Architects and developers need to approach this danger cautiously, making sure they do not compromise databases' integrity in their zeal to move to cloud computing.

3.5. Data segregation:

Multi-tenancy is one of the major characteristics of cloud computing. As a result of multi-tenancy multiple users can store their data using the applications provided by SaaS. In such a situation, data of various users will reside at the same location. Intrusion of data of one user by another becomes possible in this environment. This intrusion can be done either by hacking through the loop holes in the application or by injecting client code into the SaaS system. A client can write a masked code and inject into the application. If the application executes this code without verification, then there is a high potential of intrusion into other's data. A SaaS model should therefore ensure a clear boundary for each user's data. The boundary must be ensured not only at the physical level but also at the application level. The service should be intelligent enough to segregate the data from different users. A malicious user can use application vulnerabilities to hand-craft parameters that bypass security checks and access sensitive data of other tenants. The following assessments test and validate the data segregation of the SaaS vendor in a multi-tenant deployment:

- SQL injection flaws
- Data validation
- Insecure storage.

Any vulnerability detected during these tests can be exploited to gain access to sensitive enterprise data of other tenants.

3.6. Data access:

Data access issue is mainly related to security policies provided to the users while accessing the data. In a typical scenario, a small business organization can use a cloud provided by some other provider for carrying out its business processes. This organization will have its own security policies based on which each employee can have access to a particular set of data. The security policies may entitle some considerations wherein some of the employees are not given access to certain amount of data. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users (Blaze et al., 1999; Kormann and Rubin, 2000; Bowers et al., 2008). The SaaS model must be flexible enough to incorporate the specific policies put forward by the organization. The model must also be able to provide organizational boundary within the cloud because multiple organization will be deploying their business processes within a single cloud environment.

3.7. Authentication and authorization

Most companies, if not all, are storing their employee information in some type of Lightweight Directory Access Protocol (LDAP) servers. In the case of SMB companies, a segment that has the highest SaaS adoption rate, Active Directory (AD) seems to be the most popular tool for managing users (Microsoft White Paper, 2010). With SaaS, the software is hosted outside of the corporate firewall. Many a times user credentials are stored in the SaaS providers' databases and not as part of the corporate IT infrastructure. This means SaaS customers must remember to remove/disable accounts as employees leave the company and create/enable accounts as come onboard. In essence, having multiple SaaS products will increase IT management overhead. For example, SaaS providers can provide delegate the authentication process to the customer's internal LDAP/AD server, so that companies can retain control over the management of users.

3.8. Data confidentiality issue:

The definitional borders of cloud computing are much debated today. Cloud computing involves the sharing or storage by users of their own information on remote servers owned or operated by others and accesses through the Internet or other connections. Cloud computing services exist in many variations, including data storage sites, video sites, tax preparation sites, personal health record websites and many more. The entire contents of a user's storage device may be stored with a single cloud provider or with many cloud providers. Whenever an individual, a business, a government agency, or any other entity shares information in the cloud, privacy or confidentiality questions arise. Some of the findings related to the confidentiality issues are:

1. Cloud computing has significant implications for the privacy of personal information as well as for the confidentiality of business and governmental information.
2. A user's privacy and confidentiality risks vary significantly with the terms of service and privacy policy established by the cloud provider. 3. For some types of information and some categories of cloud computing users, privacy and confidentiality rights, obligations, and status may change when a user discloses information to a cloud provider.
4. Disclosure and remote storage may have adverse consequences for the legal status of protections for personal or business information. 5. The location of information in the cloud may have significant effects on the privacy and confidentiality protections of information and on the privacy obligations of those who process or store the information.
6. Information in the cloud may have more than one legal location at the same time with differing legal consequences.
7. Laws could oblige a cloud provider to examine user records for evidence of criminal activity and other matters. 8. Legal uncertainties make it difficult to assess the status of information in the cloud as well as the privacy and confidentiality protections available to users.

In an electronic environment, the Electronic Communications Privacy Act of 1986 (ECPA) provides some protections against government access to electronic mail and other computer records held by third parties. The privacy protections available under ECPA for the wide range of cloud computing activities are difficult to predict. Indeed, simply identifying all cloud computing applications would be a significant challenge by itself. Factors that may affect the proper applications of ECPA to cloud computing activities include

1. The precise characterization of the activity as a communication or as a storage, complicated by the recognition that an activity can move from being a communication to being store communication depending on time and possibly other factors.
2. Whether the information in question is content or non-content (e.g., header or transaction information).
3. The terms of service established by the cloud provider.
4. Any consent that the user has granted to the provider or others.
5. The identity of the service provider, for example, if the cloud provider is itself a government agency, the provider's obligation would be different from those of a non-governmental cloud provider, and the rights of users would be different.

3.9. Availability:

The SaaS application needs to ensure that enterprises are provided with service around the clock. This involves making architectural changes at the application and infrastructural levels to add scalability and high availability. A multi-tier architecture needs to be adopted, supported by a load-balanced farm of application instances, running on a variable number of servers. Resiliency to hardware/software failures, as well as to denial of service attacks, needs to be built from the ground up within the application. At the same time, an appropriate action plan for business continuity (BC) and disaster recovery (DR) needs to be considered for any unplanned emergencies. This is essential to ensure the safety of the enterprise data and minimal downtime for enterprises. With Amazon for instance, the AWS API endpoints are hosted on the same Internet-scale, world-class infrastructure that supports the Amazon.com retail site. Standard Distributed Denial of Service (DDoS) mitigation techniques such as synchronous cookies and connection limiting are used. To further mitigate the effect of potential DDoS attacks, Amazon maintains internal bandwidth that exceeds its provider-supplied Internet bandwidth. These assessments test and validate the availability of the SaaS vendor.

- Authentication weaknesses
- Session management weaknesses.

IV. CONCLUSION

As described in the paper, though there are extreme advantages in using a cloud-based system, there are yet many practical problems which have to be solved. Cloud computing is a disruptive technology with profound implications not only for Internet services but also for the IT sector as a whole. Still, several outstanding issues exist, particularly related to service-level agreements (SLA), security and privacy, and power efficiency. As described in the paper, currently security has lot of loose ends which scares away a lot of potential users. Until a proper security module is not in place, potential users will not be able to leverage the advantages of this technology. This security module should cater to all the issues arising from all directions of the cloud. Every element in the cloud should be analyzed at the macro and micro level and an integrated solution must be designed and deployed in the cloud to attract and enthrall the potential consumers. Until then, cloud environment will remain cloudy. An integrated security model targeting different levels of security of data for a typical cloud infrastructure is under research. This model is meant to be more dynamic and localized in nature. My research questions will center on application and data security over the cloud, and I intend to develop a framework by which the security methodology varies dynamically from one transaction/communication to another. One of the pieces of the framework might be focused on providing data security by storing and accessing data based on meta-data information. This would be more like storing related data in different locations based on the meta-data information which would make information invaluable if a malicious intent user recovers it. Keeping this as a core concept I am doing research on a framework which would be practical. Another piece of the framework would be providing 'Security as a Service' to the applications by providing security as a single-tier or a multi-tier based on the application's requirement and addition to it, the tiers are enabled to change dynamically making the security system less predictable. This research is based on the conceptualization of the cloud security based on real world security system where in security depends on the requirement and asset value of an individual or organization. For example, a normal human does not require personal security but a well known personality needs a body guard, an organization needs a set of security persons and a state or country have their mass military to safe guard their assets. The intense of security is directly proportional to the value of the asset it guards. In a cloud where there are heterogeneous systems having a variation in their asset value, a single security system would be too costly for certain applications and if there is less security then the vulnerability factor of some applications like financial and military applications will shoot up. On the other side, if the cloud has a common security methodology in place, it will be a high value asset target for hackers because of the fact that hacking the security system will make the entire cloud vulnerable to attack. In such a scenario, if customized security is provided as a service to applications, it would make sense. Though there are many practical concerns regarding to dynamic security and data storage based on meta-data information my research is much concentrated to derive a framework which targets these concepts and provide a practical solution.

REFERENCES

[1] Amazon. Amazon Elastic Compute Cloud (EC2), 2010 /http://www.amazon.com/ ec2/S [accessed: 10December2009].
[2] Attanasio CR.Virtual machines and data security .In: Proceedings of the workshop on virtualcomputersystems.NewYork,NY,USA:ACM;1973.p.206–9.
[3] Auger R.SQL Injection, 2009 http://projects.webappsec.org/SQL-InjectionS [accessed on:15February2010].
[4] Basta A,HaltonW.Computer security and penetrationtesting. Delmar Cengage Learning 2007.
[5] Bernard Golden.Definingprivateclouds, 2009 /http://www.cio.com/article/ 492695/
[6] Defining_Private_Clouds_Part_OneS [accessed on:11January2010].
[6] Clavister. Security in the cloud, Clavister White Cloud Security Alliance. Guidance for identity & access management V2.1,2010a /http://www.cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdfS [accessed on:9May2010].
[7] Bowers KD, JuelsA, OpreaA.HAIL:ahigh-availabilityandintegritylayerforcloud storage, CryptologyePrintArchive,Report2008/489,2008 /http://eprint.iacr. org/S [accessed on:18October2009].
[8] Choudhary V.Software as a service: implications for investment in software development. In: International conference on system sciences,2007,p.209
[9] Cloud Security Alliance. Security best practices for cloud computing, 2010b /http://www.cloudsecurityalliance.orgS [accessed on:10April2010]. Coope

BIBILOGRAPHY

CH.Deepika is from HYDERABAD, TELANGANA. Completed M.TECH in CSE with specialization (COMPUTER SCIENCE & ENGINEERING) from Hyderabad Institute of Technology & Management affiliated by JNTUH.Currently working as Assistant professor in CSE department in Vidya Jyothi Institute of Technology, Hyderabad from 2014. Her Areas of research interests include Data Mining, Networking , Android & Network security.

P.Swetha is from HYDERABAD, TELANGANA. Completed M.TECH in CSE with specialization CSE from Vidya Vikas Institute of Technology affiliated to JNTUH in 2009.Currently .she is working as an Assistant professor in CSE department at Vidya Jyothi Institute of Technology, Hyderabad from 2014. Her areas of research interests include Data Mining, Networking, Android & Network security,Cloud Computing

CH. SREEDHAR is from HYDERABAD, ANDHRAPRADESH. Completed M.TECH in ECE with specialization (VLSI SYSTEMS DESIGN) from Kshatriya college of engineering affiliated by JNTUH in 2011and B.TECH in ECE from Aizza College of Engineering & technology affiliated by JNTUH in 2006. Currently he is working as an Assistant professor in ECE department at nishitha of Engineering & Technology, Hyderabad from 2007. His areas of research interests include Wireless&Mobilecommunications,Digitalsignalprocessing, Image processing, Telecommunications, communication systems, Signal processing, embedded systems, network security.

