Bigdata Driven Cloud Security: A Survey

Raja K,1 Sabibullah Mohamed Hanifa²

Research Scholar, PG & Research Department of Computer Science,
Sudharsan College of Arts & Science, Pudukkottai – 622 104. Tamilnadu- India
E-mail Id: justmailtoraja@gmail.com, Mobile: +91-9842613188

Associate Professor & Dean, PG & Research Department of Computer Science,
Sudharsan College of Arts & Science, Pudukkottai – 622 104. Tamilnadu- India
E-mail Id: manavaisafi@yahoo.com, Mobile: +91-9443592702

Abstract: Cloud Computing (CC) is a fast-growing technology to perform massive-scale and complex computing. It eliminates the need to maintain expensive computing hardware, dedicated space, and software. Recently, it has been observed that massive growth in the scale of data or big data generated through cloud computing. CC consists of a front-end, includes the users’ computers and software required to access the cloud network, and back-end consists of various computers, servers and database systems that create the cloud. In SaaS (Software as-a-Service - end users to utilize outsourced software, PaaS (Platform as-a-Service- platform is provided) and IaaS (Infrastructure as-a-Service- physical environment is outsourced), and DaaS (Database as-a-Service-data can be housed within a cloud), where leading / traditional cloud ecosystem delivers the cloud services become a powerful and popular architecture. Many challenges and issues are in security or threats, most vital barrier for cloud computing environment. The main barrier to the adoption of CC in health care relates to Data security. When placing and transmitting data using public networks, cyber attacks in any form are anticipated in CC. Hence, cloud service users need to understand the risk of data breaches and adoption of service delivery model during deployment. This survey deeply covers the CC security issues (covering Data Security in Health care) so as to researchers can develop the robust security application models using Big Data (BD) on CC (can be created / deployed easily). Since, BD evaluation is driven by fast-growing cloud-based applications developed using virtualized technologies. In this purview, MapReduce [12] is a good example of big data processing in a cloud environment, and a model for Cloud providers.

Keywords: Cloud Computing, Cloud Service Delivery models, Cloud Security, Security Issues, Data Security, Cloud Providers, Cloud assisted-Big data models, Big Data, Hadoop MapReduce, Health Care
1. Introduction

Cloud Computing (CC) has emerged as one of the major shifts in recent Information and Communication age (ICT). Cloud Computing (CC) Security is new emerging area in computer security which refers to set of policies, controls and encryption primitives to protect online data, system application and infrastructure. It is accomplished on the top of Gartner’s list of the ten most disruptive technologies of the next years [1]. The US National Institute of Standards and Technology (NIST) describes the definition of CC technology as; “a model for enabling convenient on demand network access to a shared pool of configurable computing resources (offered by third party vendors, called Cloud Service Providers) i.e., Networks, servers, storage, applications, and services, can be rapidly provisioned and released with minimal management effort or service provider interaction”. Main concern in adapting cloud computing is its security aspects. i.e., basic building blocks for secure systems by way of adapting confidentiality, data integrity and availability. It is critical and can cause the cloud security and privacy when outsourcing the data and business application to a third party cloud. Cloud service users need to understand the risk of data breaches in the cloud environment. Authors [2], [3] proposed security solutions for various data security challenges. The communication between the cloud environment and external world is facilitated either by the Graphical User Interface (GUI) or by the APIs, made available by the service providers. Security is one the major issues which hamper the growth of cloud and use of Big data in cloud environment [4]. Security for big data on cloud is most exciting domain that posing so many security issues, includes; Network security, Information security, Application level Security and Data security privacy [5]. Security and privacy issues are magnified by velocity, volume, and variety of big data, such large scale cloud infrastructures, diversity of data sources and formats streaming nature of data acquisition, and high volume inter-cloud migration. Computing and Big Data are conjoined. Big data is eliciting attention from the academia, government and industry [36]. Moreover it is transforming health care, science, engineering, finance, business and eventually, the society. Google’s Map Reduce frame work and Apache Hadoop are the defacto software systems for big data applications

2. Cloud Computing Model

Cloud Computing (CC) is a model for enabling convenient, on-demand network access, to a shared pool of configurable resources like networks, servers, storage, applications, and services [6], [7].

2.1 Cloud Service Delivery Models & related Security Issues

Cloud computing utilizes three delivery models by which different types of services are delivered to the end user. The delivery models are SaaS, IaaS, and PaaS [8], [9].

SaaS: It is repository-rich and widely used and popular cloud model, offering services for more than one decade. It replaces the applications running on PC onto the cloud computing environment. The service repository covers a wide range of simple to complex services. It provides GUI interaction to the user for service. Some of the CSPs are Google E-Mail, Google Doc etc.,

Security Issues: To secure enterprise data, a strong encryption techniques and fine grain based access control are to be needed. Data flow from the enterprise to the SaaS application and SaaS storage should be secured to protect Man-in-the-middle attack, IP spoofing and packet sniffing. It is achieved by network traffic encryption techniques like secure socket
layer (SSL) and Transport Layer Security (TLS). Multiple users’ data and multi-tenancy are stored at the same location. Prevention of intrusion can be achieved by VM placement.

**IaaS:** It deals with the delivery of computing resources such as servers, storage, network, and other computing resources in the form of virtualized systems, which can be accessed through the internet. It offers the infrastructure as-a-service, to execute appropriate applications; it can be combined or layered to derive customized environment with various building blocks. Popular IaaS cloud models are *Amazon Web Services (AWS), Rackspace etc.,*

**Security Issues:** Associated issues must be addressed by providers to minimize the threats arise from creation, communication, monitoring, modification and mobility. In virtualization, user can create, copy, share, migrate and roll back Virtual Machines (VM), allows running variety of applications. Virtual Machine Monitor (VMM) is responsible for VM isolation (VM security).

**PaaS:** It abstracts the infrastructures and supports a set of application program interface to cloud applications. The CSP is responsible to provide the risk free and robust environment for software product development. Popular examples of PaaS are *Google App Engine, Acquia.com, Force.com etc.,*

**Security Issues:** It depends on a secure and reliable network and secure web browser. PaaS security comprises of two types: 1. Security of the PaaS platform itself. 2. Security of customer applications deployed on a PaaS platform.

**DBaaS:** It is getting popularity recently, assures the shift of data management related responsibilities. It offers a shared, a self-service model, elasticity to scale out and scale back database resources and charge-back based on database usage. Some of data related operational burdens include upgrade, provisioning, failover, management, configuration, seamless scaling, performance tuning, backup, privacy, access control etc., In this service model, the full access to a complex database can be achieved through very simple service calls only. Providers are *Amazon RDS and Microsoft SQL Azure.*

### Table 1: Security issues in cloud service delivery models

| Cloud Applications | SaaS | PaaS | IaaS |
|--------------------|------|------|------|
| **Data Security**  | Encryption | Application interface security for developing coding, deploying and testing. | Application interface security for VM management – VM security |
| **Techniques**     |       |       |      |
| Network Security   | SSL/TLS |       |      |
| Data Locality      | SLA   |       |      |
| Data Segregation   | VM placement |       |      |
| Data Access        | ACL   |       |      |
| Web Application Security | Firewall |       |      |

Where SSL is Secure Socket Layer and TLS is Transport Layer Security

Table 1 explains the security issues in different cloud service delivery models. Data access risk can be addressed by incorporating specific access policies in the SaaS application itself. Web application security addresses the programming interface design through which virtualized system and resources are accessed [10]. PaaS facilitates deployment of cloud-based applications as a service, without the cost of buying and maintaining the
underlying hardware and software. CSP should ensure there is no security hole in the virtual machine monitor [10].

2.2 Types of cloud / Cloud Deployment models

The following four types of cloud deployment models classified based on the scope of accessibility and spatial location.

1. **Public cloud** (Off-site infrastructure over the Internet): It is open to end-user (general public), or a cluster of organizations, who has the Internet availability. This system is hosted, managed, and owned by an organization selling cloud services [11]. It offers high efficiency and shared resources with low cost. The analytics services and data management are handled by the provider and the QoS (e.g., privacy, security and availability). Organizations can leverage these clouds to carry out analytics with a reduced cost or share insights of public analytics results. Leading vendors include AWS and Rackspace.

2. **Private cloud** (On-site Private network / infrastructure): It is a proprietary environment cloud, can be accessed only by a restricted group of users. There are two types if private clouds [11]. 1) Private internal cloud [Organization acquires the necessary hardware and maintains it for itself]. 2) Private external cloud. Example: Privately owned data center secured by firewall. [Organization pays a cloud provider to provide this as a service]

3. **Hybrid cloud**: Here, the private services run on a public cloud with a restricted access through a Virtual Private Network (VPN) system. The cloud infrastructure is a combination of two or more or the above models. The clouds composing a hybrid cloud remain unique entities and are bound together by technology allowing communication between the clouds [11].

4. **Community cloud**: It allows the cloud infrastructure to be used by a specific community of organizations or consumers sharing common concerns. Community clouds can be viewed as an intermediate form balancing the other clouds like private and public. It could be managed and hosted internally or externally by third party vendors [11].

2.3 Cloud characteristics

The cloud security alliance [8] has summarized five essential characteristics.

|   | 1. On-demand self-service | CSP provides computing capabilities to the consumer as and when needed automatically. |
|---|----------------------------|-------------------------------------------------------------------------------------|
| 2. | Broad Network access       | Services can be accessed through standard mechanisms by heterogeneous thin or thick client platforms like mobile phones, tablets, laptops, and workstations. |
| 3. | Resource Pooling           | Computing resources (different physical and virtual resources) are pooled to serve multiple consumers using multi-tenant model. Examples of resources includes; storage, processing, memory, network bandwidth and virtual machines. |
| 4. | Rapid Elasticity           | Capabilities can be elastically provisioned and released automatically, to scale rapidly out-ward and in-ward based on the demand. |
| 5. | Measured Service           | The service purchased by customers can be quantified and measured. Resource usage will be monitored, controlled, metered and reported. |

Confidentiality refers to any authorized parties having access to protected data. Customer’s data and computational task are to be kept confidential from both cloud provider and other
customers [3]. Data Integrity refers that data can be modified only by authorized parties or in authorized ways. It protects data from unauthorized deletion, modification or manipulation. i.e., data lost, altered, or compromised should be detected. Also, data should be honestly stored on cloud servers, and any violations must be detected. Potential security threats and mitigation strategies (Refer Table 2) in cloud security and data security solutions are explained in Table 3.

### Table 2: Cloud security issues and mitigation strategies

| Cloud Security | Network Security | Data Security |
|----------------|------------------|---------------|
|                | Firewall for VM isolation, Data transfer security | Confidentiality – Cryptography – to secure sensitive data |
|                |                  | Integrity -- Erasure code |
|                |                  | Availability -- Redundancy |
| Interfaces - Authentication | API Programming Interfaces: | SaaS (User Access, Control, Configuration) |
|                |                  | PaaS (Coding, Deploying, Testing) |
|                |                  | IaaS (VM Management) |

| Legal Issues | Visualization | Compliance | Governance |
|--------------|---------------|-------------|------------|
|              | VM Isolation, VM vulnerabilities, Data Leakage or Cross VM attacks | Service Level Agreements (SLA), Audit, Service Conformity | Lock-in, Data Control, SLA |

### Table 3: Data Security vulnerabilities and solutions

| Data Security | Confidentiality | Integrity | Computational Security |
|---------------|-----------------|-----------|------------------------|
|               | Cryptographic techniques, Proxy re-encryption, Erasure Code, VM Isolation | Distributed Erasure Code, Provable Data Possession, Proof of Retrievability Homomorphic Tags | It is a Fundamental service enabled within the cloud paradigm. Fully Homomorphic Encryption (FME), Searchable Encryption |

### 2.4 Building blocks for secure systems

In security, basic building blocks for secure systems are confidentiality, integrity and availability. CC security is a new emerging area in computer security that refers to set of policies, controls and encryption primitives to protect online data, system application and infrastructure for cloud computing. Security issues in CC include application level security, network level security, information security, and data privacy. Cloud security has to implement many different type of control such as deterrent control, preventive control, detective control and corrective controls for safeguard of its security architecture. Cloud computing comes with numerous possibilities and challenges simultaneously. Security is considered to be a critical barrier for CC in its path to success as a challenge. Security and Privacy both are concerns in CC due to the nature of such computing approach. The security issues for CC are not related to the technical and direct security breach only; a number of social inconsistencies might also be resulted even without any “hard breach” having taken
place. The security issues in CC are somewhat sensitive and crucial on the basis of sociological and technological viewpoints. The technological inconsistency results in security breach in CC might lead to significant sociological impacts. Epistemological factors are also to be considered as it gives equal importance in security issue. The below table depicts the details on nature of issue and its reason behind it.

2.5 Methods supported by Cloud

CC has leveraged a collection of existing techniques, such as Data Center Networking (DCN), Virtualization, Distributed storage, MapReduce, Web applications and services etc.,

1. Modern data center:
2. Virtualization:
3. MapReduce: It is a programming framework, supports distributing computing on mass data sets. Large data set breaks into small blocks that are distributed to cloud servers for parallel computing [12], [11]. It speeds up the batch processing on massive data sets.

| Table 4: Type of security / threats and its causes |
|---------------------------------------------------|
| **Type of Security / Threats** | **Reason behind Security / Threat** |
| Confidentiality, Availability and Integrity [13] | Generalized categories where security concerns falls in cloud environment |
| Security threats in cloud environment[14] | Database, virtual servers, network to O.S, Load Balancing, Memory Management, Concurrency Control |
| Threats for a cloud infrastructure[13] | Applicable to both data and infrastructure |
| Potential & unavoidable sec. threats in cloud users[15] | Data segregation and session hijacking |
| Level of abstraction & dynamism in scalability[15] | Results in poorly defined security or infrastructural boundary |
| Privacy and its underlying concept[15] | May lead to security breach-cloud services in specific contexts. |
| Data loss and various botnets [16],[17] | It breach security of cloud servers |
| Security in the data-centers of cloud providers[18] | Lead to security issues as a single physical server would hold many client’s data |
| Storage security at the CSPs data centers[19] | Directly linked with the security of the cloud services |
| Traditional security risks[13] | Added degree of potency in cloud infrastructure – a quite challenge in success of CC |
| Data Location[20] | Crucial factor in CC security |
| Location Transparency[20] | It is security threat and prominent flexibility in CC |
| Cloud Users’ personal Data Security (DS)[21],[22] | Crucial concern in CC |
| Customers’ personal or business DS [23] | Strategic policies of the cloud providers are of highest significance as the technical security solely not adequate |
| Trust (Trust establishment)[24] | It is not a technical issue but security concern directly related to credibility and authenticity of CSP. Some of the influential soft factors like automation management, human factors, processes and policies are driven by security issues. |
| All kinds of attacks – applies to cloud based services[25] | Man-in-the-middle attack, phishing, eavesdropping, sniffing and other similar attacks |
Distributed Denial-of-Service (DDoS) \[25\]  | Major attack in CC infrastructure and also a potential problem
---|---
Security of VM \[13\][\[26\]  | It will define the integrity and level of security of a cloud environment.
Accounting & Authentication\[27\]  | Part of security concerns in CC
Using specific type of O.S \[17\]  | It may pose security threat or security risk
Allocation of responsibilities among the parties involved in CC infrastructure \[17\]  | Result in experiencing inconsistency lead to security vulnerabilities
Insider-attack in network scenario \[17\]  | Valid threat for CC
Security tools or other kinds of software used in cloud environment\[28][\[29\]  | Lead to security loopholes and pose security risks to cloud infrastructure itself.
API and Spammers-with third party vendors \[28\]  | Threats to cloud environment
Huge amount of data transfer \[30\]  | Adapted communication technology becomes a security concern
Broadcast nature of some communication technology\[31\]  | Core concern of security issue
Physical and virtual resources in cloud environment\[32\]  | Pose different level of security issues – having no sophisticated authentication mechanism to address security threat
Virtualized resources\[33\]  | Intrusion related security concerns
Cloud portability\[34\]  | May bring severe degree of API based security threats
Using cloud products or services \[35\]  | Lead to security concerns for the consumers

3. Cloud Computing in Health Care – Future Potential

3.1 Health Care (HC) related Cloud Services

The following cloud services are specially relates with health care domain.
- Cloud-Based Analytics as-a-service (CLaaS)
- Hadoop as-a-service (HDaaS)
- Cloud as-a-service (CaaS)
- Brain segmentation as-a-service (BSaaS)
- Physical Threapy as-a-service (PTaaS)
- Biometric Authentication as-a-service (BioAaaS)

3.2 Cloud-Assisted Big Data Models

It provides efficient and most accurate solutions of complex big data problems. Some of the available models are;
1. Cloudra (Cloud based)
2. Cloudant (Cloud based)
3. CloudKit (Cloud based)
4. Cloud Datastore (Cloud based)
5. Datameer (Cloud based) - Provides HDaaS platform
6. PiCloud (Cloud based)
7. LightCloud (Non-cloud)

3.3 Use of CC infrastructure in BDA applications

Recently the use of CC has become epidemic in healthcare. Wang et al. introduced \[37\] some BD applications in HC domain including large datasets for Health Information
Systems (HIS), and CDSS, Medical Body Area Networks (MBANs). They offered cloud computing infrastructures for designing and developing BD analytics.

3.3.1 HMS based CC [37]
Microsoft Health Vault, Dossia, and Mphrx are some public health management systems based on CC.

3.4 Data security in CC –HC applications
The main barrier to the adoption of CC in health care relates to Data security [40]. The Data Security risks in the use of IT are hacker attacks, network breaks, natural disasters, public management interface, poor encryption key management, and privilege abuse [38]. However, the current cloud providers are better equipped to provide much better security than the on-premises security [39].

3.5 Task of Cloud Computing for Big Data
CC and BD paradigm is emerged to address the data-oriented challenges. CC and BD are conjoined. BD provides an ability to use commodity computing to process distributed queries across multiple datasets. CC provides the underlying engine through the use of Hadoop, a class of distributed data-processing platforms. BD utilizes distributed storage technology based on cloud computing rather than local storage attached to a computer or electronic device. Big data evaluation is driven by fast-growing cloud-based applications developed using virtualized technologies. Therefore, CC not only provides facilities for the computation and processing of BD but also serves as a service model. Table 5 shows the alliance of big data cloud providers. MapReduce [12] is a good example of big data processing in a cloud environment and a popular CC framework. It allows for the processing of large amounts of datasets stored in parallel in the cluster. MapReduce, is the preferred computation model of cloud providers [41]. It is evident that from the paper [42], cited many research issues that can be resolved by using BD on CC atmosphere.

Table 5: Alliance of several big data cloud platforms

| BD Storage | Google       | Microsoft | Amazon | Cloudra          |
|------------|--------------|-----------|--------|------------------|
|            | Google cloud services | Azure     | S3     |                  |
| MapReduce  | AppEngine    | Hadoop on Azure | Elastic MapReduce(Hadoop) | MapReduce YARN |
| BD Analytics | BigQuery    | Hadoop on Azure | Elastic MapReduce (Hadoop) | Elastic MapReduce(Hadoop) |
| NoSQL      | AppEngineStore | TableStorage | DynamoDB | Apache Accumulo |
| Relational DB | Cloud SQL  | SQL Azure | MySQL or ORACLE | MySQL or ORACLE, PostgresSQL |
| Streaming Processing | Search API | Streamlight | - | Apache Spark |
| Machine Learning | Prediction API | Hadoop+Mahout | Hadoop+Mahout | Hadoop+Oryx |
| Data Sources | Few Sample Datasets | Windows Azure market place | Public Datasets | Public Datasets |
| Data Import | Network | Network | Network | Network |
4. Conclusion

Security issues could brutally affect cloud infrastructures and also a non-compromising constraint. Robust, consistent and integrated security models for BD on cloud computing could be the right path of motivation in ongoing cloud investigation. Research endeavor on “robust security models” for CC (exclusively security met health care applications) scenarios is the most prioritized factor for winning cloud based infrastructure development and deployment. Since, cloud is able to provide at-rest analytics (i.e., retrospective analysis) for stored data. This domain gives much potential exploration area to the researchers who are interested in health care [43][44].

References
[1] Gartner top ten disruptive technologies for 2008 to 2012. “Emerging trends and technologies road show”. Technical report.Gartner, 2008.
[2] K.Ren, Cong Wang and Q.Wang, “Security challenges for the Public cloud, Internet Computing”, IEEE 16(1): 69-73, 2012, DOI: 10.1109/MIC.2012
[3] Z. Xiao and Y. Xiao, “Security and Privacy in Cloud computing, Communications Surveys and Tutorials”, IEEE 15(2): 843-859,DOI:10.1109/SURV.2012.060912.00182,2013
[4] Suren Kumar Shau, Lambodar Jena, Santhosh Satapathy, “Big Data Security issues and challenges in Cloud Computing Environment”, International journal of Innovation in Engineering and Technology (IJIET), Volume 6, Issue 2, 297-306, 2015
[5] Prof. ChetanAndhare, Prof. ShubhangiSonone, ”Survey on Security Primitives in Big Data on Cloud Computing”, International Journal of Innovative Research in Computer and Communication Engineering (IJRCCE), Vol.4 (3),2016
[6] J.Geehan, 2008, Twenty one experts define cloud computing virtualization. http://virtualization.sys-con.com/node/612375
[7] R,Buyya, C.S. Yeo., S.Venugopal, J.Broberg., and I.Brandic, , “Cloud computing and emerging IT Platforms”: Vision, Hype, and Reality of delivering computing as the 5th Utility, Future Generation Computer Systems, 25, 599-616, 2009.
[8] Cloud Security Alliance (CSA), “Top Threats to CC, V1.0”, March 2010. www.cloudsecurityalliance.org/se2010.html
[9] L.Youseff, M. Butrico and D. Da Silva, “ Toward a Unified Ontology of cloud computing, Proc. of the Grid Computing Environments Workshop”, pp: 12-16, DOI:10.1109/GCE.2008.4738443,2008
[10] N.Gonzalez, C.Miers, F.Redigolo, T.Carvalho, M.Simplicio and M.Pourzandi, “A quantitative analysis of current security concerns and solutions for cloud computing”, Cloud computing technology and Science (CloudCom), IEEE 3rd Intl., Conf. on pp:231-238, November 29, 2011 – December 1, 2011.
[11] D. Zissis and D. Lekkas “Addressing Cloud Computing Security Issues”, Future Generation Computing Systems, pp: 583-592, 2012
[12] J.Dean and S. Ghemawat, “MapReduce simplified data processing on large clusters”. ACM communication, 107-113, DOI:10.1145/1327452.1327492,2008
[13] Agarwal, A. and Agarwal, A. ” The Security Risks Associated with Cloud Computing”. International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS), 257-259,2011.
[14] Hamlen, K., Kantarcioğlu, M., Khan, L. and Thuraisingham, V. “Security Issues for Cloud Computing”. International Journal of Information Security and Privacy, 4(2), 39-51. doi: 10.4018/jisp.2010040103,2010.
[15] Chen, D. and Zhao, H. “Data Security and Privacy Protection Issues in Cloud Computing”. International Conference on Computer Science and Electronics Engineering, 647-651. doi: 10.1109/ICCSEE.2012.193,2012.
[16] Kuyoro, S.O., Ikibunle, F. and Awodele, O."Cloud Computing Security Issues and Challenges. International Journal of Computer Networks", 3(5), 247-255,2011

[17] Oigigau-Neamtiu, F. "Cloud Computing Security Issues. Journal of Defense Resource Management", 3(2), 141-148,2012.

[18] Okuhara, M., Shiozaki, T. and Suzuki, T. "Security Architectures for Cloud Computing". FUJITSU Science Technology Journal, 46(4), 397–402,2010.

[19] Mircea, M."Addressing Data Security in the Cloud. World Academy of Science, Engineering and Technology", 66, 539-546,2012.

[20] Teneyuca, D. " Internet cloud security: The illusion of inclusion. Information Security Technical Report", 16, 102-107. doi:10.1016/j.istr.2011.08.005,2011.

[21] Joint, A., Baker, E. and Eccles, E. "Hey, you, get off of that cloud? Computer Law & Security Review", 25, 270–274. doi:10.1016/j.clsr.2009.03.001,2009

[22] Ismail, N. "Cursing the Cloud (or) Controlling the Cloud? Computer Law & Security Review", 27, 250–257. doi:10.1016/j.clsr.2011.03.005,2011.

[23] Joint, A. and Baker, E. "Knowing the past to understand the present e issues in the contracting for cloud based services". Computer Law & Security Review, 27, 407 - 415. doi:10.1016/j.clsr.2011.05.002,2011.

[24] Abbadi, I.M. and Martin, A. “Trust in the Cloud. Information Security Technical Report", 16, 108-114. doi:10.1016/j.istr.08.006,2011.

[25] Dou, W., Chen, Q. and Chen, J. “A confidence-based filtering method for DDoS attack defense in cloud environment”. Future Generation Computer Systems, 29, 1838–1850. doi:10.1016/j.future.2012.12.011,2013.

[26] Rashmi, Sahoo, G. and Mehfuz, S. “Securing Software as a Service Model of Cloud Computing: Issues and Solutions”. International Journal on Cloud Computing: Services and Architecture, 3(4), 1-11. Doi: 10.5121/ijccsa.2013.3401,2013.

[27] Lee, K. " Security Threats in Cloud Computing Environments. International Journal of Security and Its Application", 6(4), 25-32,2012.

[28] Bisong, A. and Rahman, S.S.M. “An Overview of the Security Concerns in Enterprise Cloud Computing”. International Journal of Network Security & Its Applications, 3(1), 30-45. doi:10.5121/ijnsa.2011.3103,2011.

[29] Singh, S. and Jangwal, T. "Cost breakdown of Public Cloud Computing and Private Cloud Computing and Security Issues ". International Journal of Computer Science & Information Technology, 4(2), 17-31,2012.

[30] Fernando, N., Loke, S.W. and Rahayu, W. “Mobile cloud computing: A survey. Future Generation Computer Systems”, 29, 84–106. doi:10.1016/j.future.2012.05.023,2013.

[31] Celesti, A., Fazio, M., Villari, M. and Puliafito, A. “Virtual machine provisioning through satellite communications in federated Cloud environments”. Future Generation Computer Systems, 28, 85–93. doi:10.1016/j.future.2011.05.021,2012.

[32] Casola, V., Cuomo, A., Rak, M. and Villano, U." The CloudGrid approach: Security analysis and performance evaluation". Future Generation Computer Systems, 29, 387–401. doi:10.1016/j.future.2011.08.008,2013.

[33] Arshad, J, Townsend, P. and Xu, J. “A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems”, 29, 416–428. doi:10.1016/j.future.2011.08.009,2013.

[34] Petcu, D., Macariu, G., Panica, S. and Craciun, C. “ Portable Cloud applications—From theory to practice “. Future Generation Computer Systems, 29, 1417–1430. doi:10.1016/j.future,2012.

[35] Svantesson, D. And Clarke, R. " Privacy and consumer risks in cloud computing. Computer Law & Security Review", 26, 391-397. doi:10.1016/j.clsr.2010.05.005,2010.

[36] Ibrahim AbakerTargio, IbrarYaqoob, Nor BandrulAnuar, SalimahMokhtar, Abdullah Gani, SameeUllah Khan, “The Rise of “Big Data on Cloud computing”: Review and open research issues”Information Systems", 47,2015.

[37] Wang L., Ranjan,J., Kolodziej,A, Zomaya,L., Alem, " Software tools and techniques for BD computing in HC clouds “, FGCS,43:38-39, 2015.

[38] A.H.M Kuo. "opportunities and challenges of cloud computing to improve health care services” of Journal of medical internet research,vol.I3,no.3,pp,e67,2011.

[39] N.J.King. and V.T.Raja, "Protecting the privacy and security of sensitive customer data in the cloud . “ Computer Law & Security Review,vol.28,no.3,pp.308-319,2012
[40] J.L. Fernandez-Aleman, I.C. Senor, P.A.O. Lozya, and A. Toval, “Security and privacy in electronic health records: A systematic literature review,” Journal of Biomedical Informatics, vol. 46, no. 3, pp. 541-562, 2013.

[41] X. Zhifeng, X. Yang, Security and privacy in cloud computing, IEEE Commun. Surv. Tutor. 15-2013.

[42] The rise of “big data on cloud computing”: Review and open research issues Ibrahim Abaker Targio Hashem, Ibrar Yaqoob, Nor Badrul Anuar, Salimah Mokhtar, Abdullah Gani, Samee Ullah Khan, Information Systems, 2015.

[43] Sabibullah M., “Prognostic Neural Network model for diabetic risks prediction”, In Proc. of IEEE International Conference on Emerging Trends in Science, Engineering and Technology, pp. 392-395, 2012.

[44] Sabibullah M., Shanmugasundaram V., Raja Priya K., “Diabetes Patient’s Risk through Soft Computing Model”, Int. Jr. of Emerging Trends & Tech. in Comp. Sci. (IJETTS), Vol. 2, No. 6, 61-65, Nov-Dec, 2013.

Author’s

**Mr. K. RAJA** received his postgraduate MCA degree in Bharathidasan University, Tiruchirappalli in 2006 and completed M.Phil (Computer Science) in the year 2008 from Vinayaka Missions University, Salem. He attended many National conferences, workshops, and seminars. His area of interest includes Cloud computing, Data mining and Big Data. At present, he is pursuing Ph.D (Computer Science) in Bharathidasan University, Tiruchirappalli.

**Dr. M. SABIBULLAH**, currently working as Associate Professor & Dean in PG & Research Department of Computer Science and has 18+ years of academic experience and 9+ years of research experience specializing in Machine Learning, Biomedical big data, Cloud computing and Health care applications. He published many research papers; participated in International Conferences. Acting as a reviewer in the International Conferences and chaired many National level computing related conferences. Now, he is very keen on harnessing research interests towards hot areas of Computer Science domain like IoT, Big Data, Cloud Computing, Health Care Predictive Analytics and Data Classification algorithms. He is a life member in various professional bodies.