Volume No 03, Special Issue No. 01, March 2015 ISSN (online): 2348 – 7550

A REVIEW OF CLOUD COMPUTING THREATS & SECURITY ISSUES

[1] Rahul Singh, [2] Punyaban Patel, [3]Preeti Singh

[1, 2, 3] Department of Computer Science & Engineering, CSIT, Durg (India)

ABSTRACT

As Cloud Computing is maturing with time, from being a buzzword & an exciting opportunity for the IT circle to becoming a real, concrete technological model for organizations & businesses which they can migrate to and take advantages of the features, freedoms & chances it offers. Anyone who aims to be successful in the near future is working on getting the most out of this promising paradigm. With most opportunities & new unexplored paths there are some risks involved. The cloud computing model is also a new avenue for the non-IT world & everyone has their doubts & concerns. Security is the biggest concern among all the people & organizations whether they are cloud users or cloud service providers. Whenever someone uploads data to a remote location either for storage or processing, there is some worry about its safety. This Paper gives study of cloud computing risks and serves as a source for threat recognition that will help cloud clients and vendors to settle on educated choices about risk relief inside a cloud environment.

Keywords – Attacks, Cloud Computing, Data Breach, DoS attack, Risk, Security, Threats, Virtualization

I. INTRODUCTION

In the recent past, cloud computing has developed from being just a promising business idea to one of the fastest growing segments of the IT industry. It is providing seemingly boundless infrastructure to store consumer data and execute programs. Today Cloud Computing is a booming deployment option for IT firms as Small and Medium Business companies are realizing the potential of the idea that simply by moving onto the cloud they can gain fast access to best business applications or remarkably improve their infrastructure resources, all at very slim costs. 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 tampering and rapid re-constitution of services [25].

Whenever a company is moving to the cloud or anyone is looking to use any of the cloud services the biggest concern is of security. The cloud service providers hold the responsibility of any problems if things go wrong, thus the providers must make sure that they get the security aspects right. According to IHS the global market for cloud computing in April 2014 was estimated at about $70 billion, and is estimated to grow to about $250 billion by 2017 [42]. 42% of IT decision makers are planning to increase spending on cloud computing in 2015, with the greatest growth in enterprises with over 1,000 employees [41]. Everybody and anybody who is going to

be successful in the next decade or so has a plan to attack the cloud. The traditional enterprise IT players, whether they're on the hardware side or on the software side, whether it's an Oracle and a Microsoft or a Cisco or an Avaya, or an HP or a Dell, has a plan to essentially address the cloud [42]. Fig.1 shows the top five estimated tech spending increases in 2015. Cloud computing comes second, behind security technologies. This graphic depicts the overall spending of the IT industry. As one would expect security is the most focused issue in the IT world at the moment. And the sub-section of Cloud Computing is also expected to follow the trend. Security is the most vital issue in the Cloud environment.

The next section acquaints the readers to the Cloud Computing Paradigm. The definitions, characteristics, service & deployment models are presented. The section after that focuses on the threats & security issues pertaining to the cloud environment. Various concerned issues & kinds of attacks are discussed.

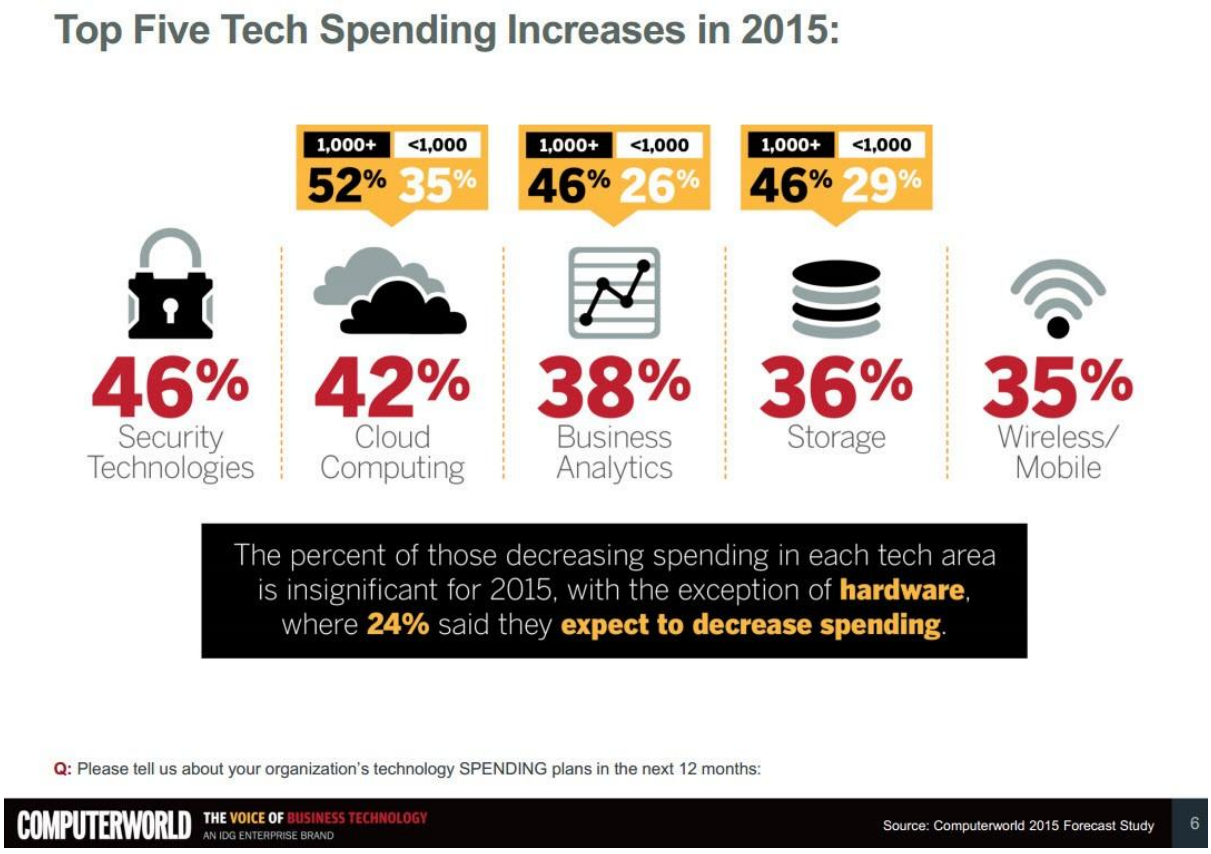

Fig. 1: Top Five Forecasted Tech Spending Trends in 2015

II. THE CLOUD COMPUTING PARADIGM

Cloud Computing is a fairly new paradigm that has made quite an impact on the world of computing. It is said to have evolved from Grid Computing, which is a model that gives the capacity to perform higher throughput processing by exploiting numerous arranged machines to model a virtual machine architecture that has the capacity appropriate procedure execution over a parallel infrastructure. Cloud computing refers to both the

applications conveyed as services over the Internet and the hardware infrastructure and programming platform in the data centres that provide those services. It gives the facility to access shared resources and common infrastructure, offering services as needed over the networked system to perform operations that meet changing business needs, and all the while, end users are unaware of the location of physical resources and devices being accessed. Fig.2 illustrates the cloud computing model.

2.1 Definitions of Cloud Computing

The term "Cloud Computing" itself doesn't hint anything about what it means to anyone who doesn't already know what it is [30]. Many experts have given many definitions of the paradigm. Armbrust et al. (2009) postulate: "Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The data center hardware and software is what we call a Cloud" [1]. According to National Institute of Standard and Technology cloud is defined as "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". This cloud model is composed of five essential characteristics, three service models, and four deployment models [20]. Vaquero et al. (2009) summarize proposed definitions and introduce a new one: "Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. The pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs" [37].

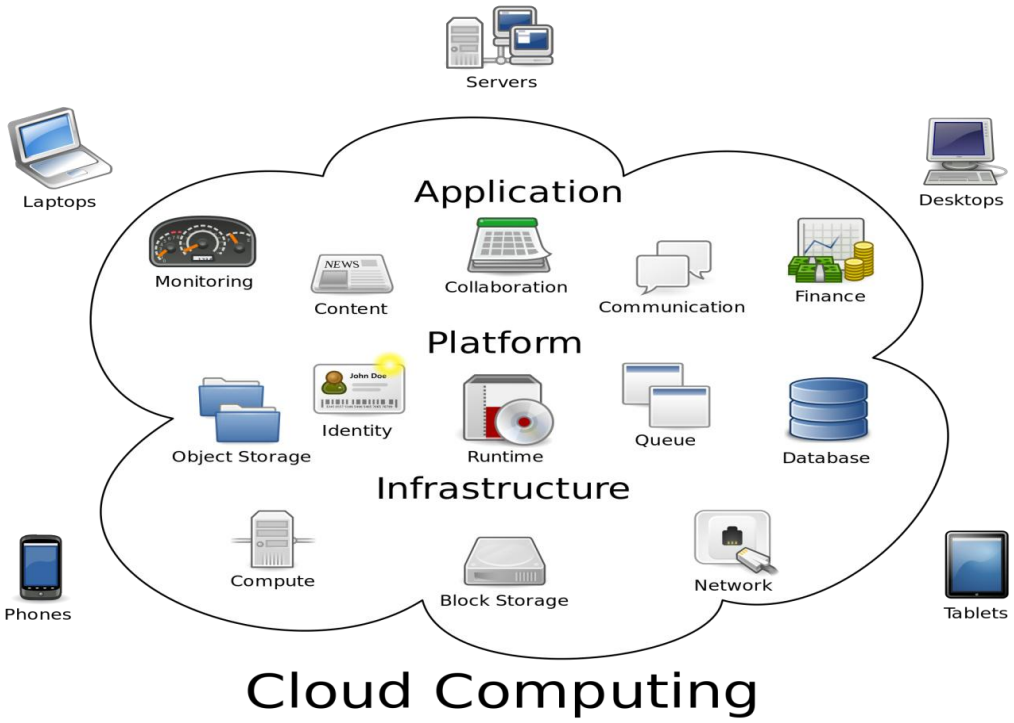

Fig. 2: The Cloud Computing Model

2.2 Essential Characteristics of Cloud Computing

- On-demand self-service: The consumer has the control over which service of the provided options he or she is going to use & how much, as and when needed without any human interaction [30].
- Broad network access: Usually the Internet is the medium for providing services. These services can be accessed through any device that has the capacity to access the internet, may it be a desktop computer, a laptop or a mobile phone.
- Resource pooling: All the computing resources of the provider are pooled together in order to serve multiple clients simultaneously. The resources, physical or virtual are assigned & revoked depending on the user demand in real time. The users have no idea about the resources being provided are located. They can be in a different country or even on a different continent [30].
- Rapid elasticity: There is a high degree of flexibility when it comes to the capabilities. They can be increased or decreased, depending on the demand. It seems to the user that there are unlimited resources at their disposal & they can use them, of-course on a pay-per-use basis.
- Measured service: Cloud systems manage & optimize the utilization of resources at some level of abstraction depending on the type of service by applying measured use of the service. This provides transparency between the provider & user of the service can be observed, kept in check & reported.

2.3 Cloud Computing Service Models

There are basically three service models in the Cloud Model, i.e. the services can be provided to the clients in three forms. These service models are discussed next. Fig.3 illustrates the service models as layers that run one – over – another & lists some examples of the available services.

- Software as a service (SaaS): In this model, the cloud client exploits programming running on the cloud supplier's foundation as opposed to on the client's own particular equipment. The applications needed are available from different customer gadgets through either a thin client interface, for example, a web program (online email), or a program interface. In SaaS administrations, the client has no power over the fundamental cloud framework, getting to applications through a web program or separate project interface. An alternate definition of XaaS (Everything as a Service) that may comprehensively be incorporated in SaaS is CaaS (Communication as a Service), which incorporates cloud administrations for messaging and Voice Over Internet Protocol (VOIP).
- Platform as a service (PaaS): In this model, the cloud clients use their own applications and information on stage devices, including programming apparatuses, having a place with and oversaw by the cloud supplier. Application designers chipping away at portable applications generally utilize cloud-based stages to create and dispatch their administrations. The cloud client does not oversee or control the hidden cloud foundation, for example, system, servers, working frameworks, or capacity, yet has control over the conveyed applications and maybe over arrangement settings for the application facilitating environment.
- Infrastructure as a service (IaaS): In this model, the cloud supplier's transforming, stockpiling, systems and other principal processing assets permit the cloud client to send and run programming, which can incorporate working frameworks and applications. The cloud client does not oversee or control the fundamental framework however has control over working frameworks, stockpiling and conveyed applications, and may have constrained control of select systems administration parts (for instance, host firewalls). Making utilization of the flexibility of IaaS for information stockpiling and transforming limit permits an association or venture to get to processing foundation in an adaptable and auspicious way.

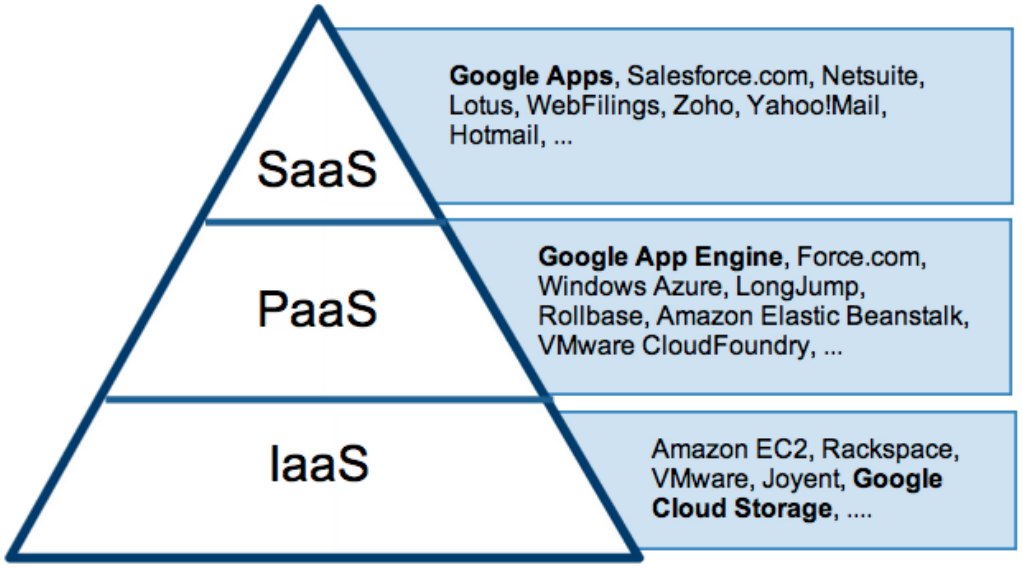

Fig. 3: Service Models in Cloud Computing

2.4 Cloud Computing Deployment Models

- Private Cloud – The cloud infrastructure is owned or leased by a single organization and is operated solely for that organization.
- Community Cloud – Several organizations that have similar polices, objectives, aims and concerns share the cloud infrastructure.
- Public Cloud – A large organization owns the cloud infrastructure and sells cloud services to industries or public.
- Hybrid Cloud – It is combination of two or more clouds. It enables data and application probability.

2.5 Benefits of Cloud Computing

Some benefits of cloud computing can be listed as:

- Reduced Cost: Organizations don't have to build the infrastructure needed for their IT needs. This reduces the cost for organizations that move to the cloud environments as they can get resources as and when needed & make payments incrementally.
- Increased Storage: Cloud storage services provide huge storage space at trifling rates. People and organizations can get as much storage they need and store much more data than on private computer systems.
- Highly Automated: The cloud users don't need to worry about software updates & don't have to sweat to keep up with the ne advances in the technology.
- Flexibility: The cloud computing model offers much more flexibility in comparison to the traditional computing methods as services can be utilized on-demand & scaled with the changing needs.

- More Mobility: People can access information & services whenever they want, wherever they are, rather than having to stay tied to their desks.
- Allows IT to Shift Focus: Experts can focus on R&D, no longer having to worry about constant server updates and other computing issues. Governments & organizations are free to concentrate on innovation.

III. THREATS AND SECURITY ISSUES

Cloud computing environment is for the most part expected as a potential expense saver and in addition supplier of higher administration quality. Security, Availability, and Reliability are the significant quality concerns of cloud administration clients, recommends that security in one of the noticeable test among all other quality challenges. Each of these models has an alternate effect on application security. There is various security issues connected with cloud computing however these issues fall into two general classes: Security issues confronted by cloud providers and security issues confronted by their clients. A discussion of the various cloud threats & security issues follows.

3.1 Abuse of Cloud Services

This threat is more of an issue for cloud service providers than cloud consumers, but it does raise a number of serious implications for those providers [23]. Cloud providers lend computing resources & services to all the clients whether they are individuals or small or enormous corporations. The clients don't have to buy and keep up a large number of servers, as cloud service providers rent them all the servers they need for moderate prices. However not all clients utilize this power as a windfall. For an attacker to gauge the encryption keys will take years with a solitary server. Yet with the assistance of a great many servers it will get to be anything but difficult to gauge the keys inside minutes.

3.2 Account Hijacking

Account or Service Hijacking incorporates assaults like phishing, extortion, and abuse of software programming. This security risk emerges because of loss of credentials. In the event that the attackers get access to your ids and passwords, they can without much of a stretch get access to your classified information and bookkeeping data. Additionally they can control or erase your information, return misrepresented data, and sidetrack your customer to some illegitimate site. To maintain a strategic distance from this, the associations or people ought to shield their passwords and certifications from being imparted in the middle of clients and administrations. Additionally legitimate verification system ought to be utilized.

3.3 Authentication and Authorization

Most companies, if not all, are storing their employee information in some type of Lightweight Directory Access Protocol (LDAP) servers [25]. 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 product and services are facilitated outside of the corporate firewall.

Numerous times client credentials are put away in the SaaS suppliers' databases and inside the corporate IT infrastructure. This implies SaaS clients must not forget to remove or disable the accounts as workers leave the organization and create/re-enable accounts as people come onboard. Fundamentally, having numerous SaaS products will expand IT administration overhead. Case in point, SaaS suppliers can give appoint the validation procedure to the client's inside LDAP/AD server, with the goal that organizations can hold control over the administration of clients.

3.4 Availability

The SaaS application needs to guarantee that clients are provided services all day and all night. This includes rolling out architectural improvements at the application and infrastructural levels to include versatility and high accessibility. A multi-level architectural design needs to be embraced, backed by load balancing techniques of utilization cases, running on a variable number of servers. Versatility to equipment/programming failures, and in addition to Denial of Service (DoS) attacks, needs to be developed starting from the earliest stage 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 [25].

3.5 Backup

The Cloud service providers need to make sure that all confidential & important information is regularly backed up to facilitate quick recovery in case of power failures or natural disasters. The backup of the data should be kept at different locations which are geographically far away from each other, thus, minimizing the chances of the same disaster or problem affecting both the original data location and the back-up location. The backup data should be updated at regular intervals. The use of effective & powerful encryption techniques is recommended to protect the backup data from accidental leakage.

3.6 Data Access

Information access issue is primarily identified with security strategies gave to the clients while getting to the information. In an ordinary situation, a little business association can utilize a cloud gave by some other supplier to completing its business forms. This association will have its own security approaches in light of which every representative can have entry to a specific set of information. The security strategies may entitle a few contemplations wherein a percentage of the workers are not offered access to certain measure of information. The cloud service model must be sufficiently adaptable to consolidate the particular approaches set forward by the association. The model must additionally have the capacity to give hierarchical limit inside the cloud in light of the fact that different association will be sending their business forms inside a solitary cloud environment.

3.7 Data Breaches

The CIOs of every organization has the hallucination of losing their sensitive internal data to their competitors. In November 2012, researchers from the University of North Carolina, the University of Wisconsin and RSA

Corporation released a paper describing the fact that if multiple virtual machines are running on a single physical server, than it may be possible to extract the private cryptographic keys used on one virtual machine by sitting on other virtual machine using side channel timing information. In a multitenant environment, if a flaw exists in a single tenant's application cloud allow an intruder to access the application of all the clients present in the environment. The impact of data breaches can be reduced by encrypting the data, but if you lose your encryption key, your data will be lost automatically. Multiple copies of data are prepared to reduce the impact of data loss but it will increase your exposure to data breaches [11].

3.8 Data Confidentiality Issue

The definitional outskirts of cloud computing are tremendously bantered about today. Cloud computing includes the offering or stockpiling by clients they could call their own data on remote servers claimed or worked by others and gets to through the Internet or different associations. Cloud computing services exist in numerous varieties, including information stockpiling locales, feature destinations, charge readiness locales, individual health record sites and numerous more. The whole substance of a client's capacity gadget may be put away with a solitary cloud supplier or with numerous cloud suppliers. At whatever point an individual, a business, a legislature office, or some other element offers data in the cloud, protection or confidentiality inquiries emerge. All this important data is very valuable & the confidentiality must be maintained.

3.9 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 [25]. Usually ACID (atomicity, consistency, isolation and durability) properties are followed during transactions to ensure the integrity of data. Enter the universe of SOA and Cloud computing, and the issue of the data integrity gets amplified considerably more, as there is a blend of on-reason and SaaS applications uncovered as administration. SaaS applications are multi-tenant applications facilitated by a third gathering. SaaS applications typically uncover their usefulness through XML based APIs (Application Program Interfaces). Additionally, in SOA based situations, numerous on-reason applications uncover their usefulness through SOAP and REST web benefits too. One of the greatest difficulties with web administrations is exchange administration. At the convention level, HTTP (Hyper Text Transfer Protocol) does not help exchanges or ensured conveyance, so the main alternative is to execute these at the API level. Albeit there are gauges accessible for overseeing information honesty with web administrations, for example, WS-Transaction and WS-Reliability, these guidelines are not yet develop and relatively few sellers have executed these. Most SaaS sellers uncover their web administrations APIs with no backing for exchanges. Additionally, every SaaS application may have diverse levels of accessibility and SLA (administration level understanding), which further muddles administration of exchanges and information respectability crosswise over numerous SaaS applications.

3.10 Data Locality

In the cloud scenario, the customer has no idea where the data is getting stored. In many a cases, this can be a problem. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in many enterprise architectures. For example, in many European and South American 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 jurisdiction, if an investigation is underway.

3.11 Data Loss

For cloud clients, data loss is a standout amongst the most concerning issue. A man lost all his personal records because of absence of data security by the cloud administration. Obviously, information put away in the cloud can be lost because of different reasons also. A coincidental or physical disaster like fire and earthquake can cause the loss of valuable data. Moreover, if a client transfer its information to the cloud in the wake of scrambling it and loses the encryption key because of any reason, the information will be lost too.

3.12 Data Security

In a conventional computing software deployment model, the delicate data of every undertaking keeps on staying inside the venture limit and is liable to its physical, coherent and staff security and access control strategies. Nonetheless, in the cloud demonstrate, the undertaking information is put away outside the venture limit, at the cloud merchant end. Therefore, the cloud vendor must embrace extra security checks to guarantee information security and anticipate ruptures because of security vulnerabilities in the application or through noxious workers. This includes the utilization of solid encryption systems for information security and fine-grained approval to control access to information. 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 [25]:

- 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.

3.13 Data segregation

Multi-occupancy is one of the significant attributes of distributed computing. As a consequence of multi-occupancy various clients can store their information utilizing the applications gave by SaaS. In such a circumstance, information of different clients will live at the same area. Interruption of information of one client by an alternate gets to be conceivable in this environment. This interruption could be possible either by hacking

through the escape clauses in the application or by infusing customer code into the SaaS framework. A customer can compose a veiled code and infuse into the application. In the event that the application executes this code without confirmation, then there is a high capability of interruption into other's information. A SaaS model ought to in this manner guarantee a reasonable limit for each client's information. The limit must be guaranteed at the physical level as well as at the application level. The administration ought to be sufficiently insightful to isolate the information from diverse clients. A malicious user can use application vulnerabilities to handcraft 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 [25]:

- SQL injection flaws
- Data validation
- Insecure storage

3.14 Denial of Service

Denial-of-service attack is like being caught in rush-hour traffic gridlock: there is no way to get to your destination, and nothing you can do about it except sit and wait [23]. As a client, administration blackouts baffle you, as well as power you to re-evaluate whether moving your discriminating information to the cloud to lessen framework expenses was truly beneficial when its all said and done. Since cloud suppliers regularly bill customers in view of the process cycles and circle space they expend, there is the likelihood that an assailant will be unable to totally thump your administration off of the net, however may at present reason it to devour so much transforming time that it gets to be excessively lavish for you to run and you will be compelled to bring it down yourself.

3.15 Identity Management and Sign-On Process

Identity management (IdM) or ID management is a broad administrative area that deals with identifying individuals in a system (such as a country, a network or an organization) and controlling the access to the resources in that system by placing restrictions on the established identities. Identity management can involve three perspectives [25]:

1. The pure identity paradigm: Creation, management and deletion of identities without regard to access or entitlements.
2. The user access (log-on) paradigm: For example: a smart card and its associated data used by a customer to log on to a service or services (a traditional view).
3. The service paradigm: A system that delivers personalized role based, online, on-demand, multimedia (content), presence based services to users and their devices.

3.16 Insecure Interfaces & APIs

The interfaces or APIs used to interact with the service providers are prone to risks by attackers [11]. Most providers strive to ensure security is well integrated into their service models, it is critical for consumers of

those services to understand the security implications associated with the usage, management, orchestration and monitoring of cloud services. Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability [23].

3.17 Insufficient Due Diligence

Cloud computing is a standout amongst the most built up IT developments. Numerous organizations being pushed to the cloud without a complete understanding of Cloud Service Provider (CSP) environment. Because of this associations are assuming obscure level of danger. By embracing cloud advancements without fitting comprehension will leave the association with number of issues. The gauge for any association to embrace this new innovation is that they must have proficient assets and perform broad interior and CSP due diligence to understand the concepts.

3.18 Malicious Insiders

A malicious insider, for example, a system programmer, in a improperly outlined cloud scenario can have access to possibly sensitive data. From IaaS to PaaS and SaaS, the malicious insider has expanding levels of access to more discriminating frameworks, and inevitably to information. Frameworks that depend exclusively on the cloud service provider (CSP) for security are at extraordinary hazard here. Regardless of the possibility that encryption is actualized, if the keys are not kept with the client and is just accessible at information use time, the framework is still defenceless against malicious insider assault.

3.19 Network Security

In a cloud deployment model, sensitive data is obtained from the enterprises, processed by the SaaS application and stored at the cloud 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 [25].

3.20 Shared Technology Issues

A trade off of an essential bit of imparted innovation, for example, the hypervisor, an imparted stage segment, or an application in a SaaS environment uncovered more than simply the traded off client; rather, it uncovered the whole environment to a capability of trade off and rupture. This defencelessness is risky on the grounds that it possibly can influence a whole cloud without a moment's delay.

3.21 Vulnerability in Virtualization

Virtualization is one of the principle sections of a cloud environment. In any case this stances significant security danger. Guaranteeing that diverse occasions running on the same physical machine are secluded from one another is a noteworthy undertaking of virtualization which is not met totally in today's situation. The other issue is the control of overseer on host and visitor working frameworks. Current VMMs (Virtual Machine Monitor) don't offer impeccable confinement. Numerous bugs have been found in all mainstream VMMs that

permit getting away from VM. Virtual machine monitor ought to be 'root secure', implying that no benefit inside the virtualized visitor environment grants obstruction with the host framework. Some vulnerability has been found in all virtualization software which can be exploited by malicious, local users to bypass certain security restrictions or gain privileges [25]. For example, the vulnerability of Microsoft Virtual PC and Microsoft Virtual Server could allow a guest operating system user to run code on the host or another guest operating system.

IV. CONCLUSION

There is no doubt what so ever that cloud computing is providing benefits to IT enterprises with its various facilities and on demand services in a cost effective manner. Every business whether big or small can benefit from moving to the clouds. But there are various challenges and security problems which everyone must consider before transferring the data to a cloud. Data Security is the biggest challenge faced by the cloud community. So the way to better nature of administration and fruitful cloud computing activities is to have a harmony in the middle of profits and the related risks. Cloud suppliers ought to include more assets and security approaches to shield themselves from noxious assaults. This paper has presented an overview of most of the issues concerning the security aspect of the cloud paradigm. As the clouds are in continual developmental phase, the researchers have a lot of challenges in handling the security threats, energy conservation, resource management, scheduling strategies, interoperability and reliability in cloud computing and make it a successful and profitable technology.

REFERENCES

[1]. Armbrust M., et al. "A View of Cloud Computing", Communications of the ACM, April 2010, vol. 53, no. 4, pg: 50-58, DOI:10.1145/1721654.1721672

[2]. Ashktorab V., Taghizadeh S.R., "Security Threats and Countermeasures in Cloud Computing", IJAIEM, ISSN 2319 - 4847, Volume 1, Issue 2, October 2012, pg: 234-245

[3]. Buyya R., Yeo C. S., Venugopal S., Broberg J., and Brandic I., "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities", in proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, HPCC'08, Dalian, China, Sept. 2008.

[4]. Buyya R., Yeo C. S., Venugopal S., Broberg J., and Brandic I., "Market-Oriented Cloud Computing: Vision, Hype, and Reality of Delivering Computing as the 5th Utility", Proceedings of the 2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid, CCGRID '09, ISBN: 978-0-7695-3622-4 DOI: 10.1109/CCGRID.2009.97

[5]. Buyya, R., Broberg, J., Goscinski, A., "Cloud Computing: Principles and Paradigms", Wiley, 2011, ISBN: 978-81-265-4125-6

[6]. Choubey R., Dubey R.,, Bhattacharjee J., "A Survey on Cloud Computing Security, Challenges and Threats", IJCSE, ISSN: 0975-3397Vol. 3 No. 3, Mar 2011, pg: 1227-1231

[7]. Dargan S., "Security Threats in Cloud Computing Environment", Journal Of Information, Knowledge And Research In Computer Engineering, ISSN: 0975 – 6760, VOLUME – 03, ISSUE – 02, pg: 619-621

[8]. Devangan K.K., Wanjari A., Dewangan S.K., "A Valued Analysis of Information Security, Threats and Solutions for Cloud Computing", IJARCSEE, ISSN: 2277 – 9043, Volume 2, Issue 9, September 2013, pg: 648-658

[9]. Dhingra M., "Cloud Data Encryption Ensuring Security", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 4 Issue 01, January-2015, pg: 62-64

[10]. Gharehchopogh F.S., Rezaei R., Maleki I., "Mobile Cloud Computing: Security Challenges for Threats Reduction", International Journal of Scientific & Engineering Research, ISSN: 2229-5518, Volume 4, Issue 3, March-2013

[11]. Gupta S., Khandelwal S., "Cloud Computing Security Threats", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 4 Issue 01, January-2015, pg:20-22

[12]. Hayes B., "Cloud computing", Communications of the ACM, July 2008, Vol. 51, No. 7, pg. 9-11, DOI: 10.1145/1364782.1364786.

[13]. Inbarani W.S., et al., "A Survey on Security Threats and Vulnerabilities In Cloud Computing", International Journal of Scientific & Engineering Research, ISSN 2229-5518, Volume 4, Issue 3, March -2013, pg: 1-4

[14]. Joshi A.G., Shele R.R., "Overview on Security Threats and Solutions in Cloud Computing", International Journal of Computer, Information Technology & Bioinformatics (IJCITB), ISSN: 2278-7593, Volume-2, Issue-2, pg: 1-5

[15]. K. Valli Madhavi et al, "Cloud Computing: Security Threats and Counter Measures", International Journal of Research in Computer and Communication technology, IJRCCT, ISSN: 2278-5841, Vol 1, Issue 4, September 2012

[16]. K.L.Neela, V.Kavitha, R.K.Ramesh, "Cloud Computing: Threats and Security Issues", IJESRT, ISSN: 2277-9655, Vol. 2 Issue 8 Aug 2013, pg: 2070-2072

[17]. Kumar P. et al. "Security Threats to Cloud Computing", International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) ISSN: 2319-4413, Volume 2, No. 1, December 2013, pg: 25-29

[18]. Lee K., "Security Threats in Cloud Computing Environments", International Journal of Security and Its Applications, Vol. 6, No. 4, October 201 2, pg: 25-32

[19]. Makkar G.D., Panwar V., "Cloud Computing Security: Risks and Threats", IJETTCS, ISSN 2278-6856, Volume 3, Issue 2, March – April 2014, pg: 111-116

[20]. Mell P., Grance T., "The NIST Definition of Cloud Computing", NIST Special Publication 800-145, September 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[21]. Muthukumar V.P., Saranya R., "A Survey on Security Threats and Attacks in Cloud Computing", Computer Science International Journal of Computer Sciences and Engineering, E-ISSN: 2347-2693, Volume-2, Issue-11, pg: 120-125

[22]. Nicho M., Hendy M., "Dimensions Of Security Threats In Cloud Computing: A Case Study", Review of Business Information Systems – Fourth Quarter 2013, Volume 17, Number 4, pg: 159-170

[23]. Raju M., Lanitha B., "Survey about Cloud Computing Threats", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014, pg: 384-389

[24]. Rot A., Sobinska M., "IT Security Threats in Cloud Computing Sourcing Model", Proceedings of the 2013 Federated Conference on Computer Science and Information Systems, pp. 1141–1144

[25]. S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Elsevier Journal of Network and Computer Applications 34 (2011), pg: 1–11

[26]. Sabahi F., "Cloud Computing Security Threats and Responses", 978-1-61284-486-2/11/pg: 245-249, ©2011 IEEE

[27]. Shah B., Vania J., "A Literature Survey on Virtualization Security Threats in Cloud Computing", International Journal of Science and Research (IJSR), ISSN (Online): 2319-7064, Volume 3 Issue 12, December 2014, pg: 1137-1140

[28]. Shaikh F.B., Haider S., "Security Threats in Cloud Computing", 6th International Conference on Internet Technology and Secured Transactions, 11-14 December 2011, Abu Dhabi, United Arab Emirates, 978-1-908320-00-1/11/pg: 214-219 ©2011 IEEE

[29]. Singh R., Patel P., "Cloud Computing vs. Grid Computing: A Comparison", in the Proceedings of ICETPITM – 2015, International Conference on Exploring Trends and Practices in Information Technology and Management, 5'Th – 6'Th January, 2015, St. Aloysius' College, Jabalpur, M.P.

[30]. Singh R., Patel P., Sahoo B., "A Compendium of Cloud Computing", International Journal of Advance Computing Technique and Applications (IJACTA), ISSN: 2321-4546, Vol. 2, No. 1 (January, 2014), pg: 073-079

[31]. Solanke V.S., Kulkarni G.A., Katgaonkar P., Gupta S., "Mobile Cloud Computing: Security Threats", Proceedings of International Conference on Electronics and Communication Systems (ICECS'14), pg: 550-553

[32]. Soofi A.A., Khan M.I., Fazal-e-Amin, "Encryption Techniques for Cloud Data Confidentiality", International Journal of Grid Distribution Computing, ISSN: 2005-4262, Vol.7, No.4 (201 4), pp.1 1 -20, http://dx.doi.org/10.14257/ijgdc.2014.7.4.02

[33]. Srivastava P., Chandan R.R., Singh R.K., "A perspective view of security threats in cloud Computing", National Conference on Challenges & Opportunities to Computer science & Information technology in Next Generation, (COTII-13),16thfeb-2013,AIMT,Lucknow

[34]. Te-Shun Chou, "Security Threats on Cloud Computing Vulnerabilities", International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3, June 2013, pg: 79-88, DOI : 10.5121/ijcsit.2013.5306

[35]. Tiwari D., Dhariwal M.K., Kesharwani A., Tehariya S.K., "Security Threats in Cloud Computing", IJMEMR, ISSN: 2320-9984 (Online), Volume 1, Issue 4, December 2013, pg: 5-12

[36]. Tiwari D., Tiwari D., "A survey ofcloud computing security threats", Proceedings of the International Conference on Cloud, Big Data and Trust 2013, Nov 13-15, RGPV, pg: 47-51

[37]. Vaquero L. M., Rodero-Merino L., Caceres J., Lindner M., "A Break in the Clouds: Towards a Cloud Definition", ACM SIGCOMM Computer Communication Review, Volume 39, Number 1, January 2009, pg: 50-55

[38]. Yadav A.R., "Identified Vulnerabilitis And Threats In Cloud Computing", IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. III (Jan – Feb. 2015), pg: 01-04

[39]. Zhang Q., Cheng L., Boutaba R., "Cloud computing: state-of-the-art and research challenges", J Internet Serv Appl (2010) 1: 7–18, Springer, DOI 10.1007/s13174-010-0007-6

[40]. Collett S., 'Forecast 2015: IT spending on an upswing", http://www.computerworld.com/article/2840907/forecast-2015-it-spending-on-an-upswing.html, accessed March 2015

[41]. Columbus L., "Roundup Of Cloud Computing Forecasts And Market Estimates, 2015", http://www.forbes.com/sites/louiscolumbus/2015/01/24/roundup-of-cloud-computing-forecasts-and-market-estimates-2015/, accessed March2015

[42]. Rebello J., IHS Technology, https://www.ihs.com/articles/videos/enterprise-cloud-computing.html, accessed March 2015