International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 4 Issue 4 || April 2015 || PP.52-63

A Detail Overview of Cloud Computing with its Opportunities and Obstacles in Developing Countries

Mohammed Humayun Kabir[1], Syful Islam[2], Md. JavedHossain[3] , Sazzad Hossain[4]
[1,2,3,4]*Dept. of CSTE, Noakhali Science and Technology University, Sonapur, Noakhali-3814, Bangladesh*

ABSTRACT*: In this modern age of science and technology, Cloud Computing has become an emerging technology that gains wide influence on information technology (IT) systems by providing a friendly environment to its user with various services such as SaaS, PaaS,, and IaaS.. The trend of frequently adopting this technology by many different organizations automatically introduced new security risk on top of inherited risk. That's why security is considered as a key requirement for a robust and feasible multipurpose solution in cloud computing models. Due to the ever growing interest in cloud computing, researchers have explicit and constant effort to evaluate the current trends in security for such technology, considering both problems already identified and possible solutions . In our entire paper, we will try to show clear presentations for every cloud computing service model currently available, and noting how they differ from each other by using head-to-head presentation table that will further clear our concept about cloud models. At the end of the paper, we will try our best to discuss and analyze the opportunities & obstacles of cloud computing in developing countries.*

KEYWORDS - *Cloud Computing, Deployment Model, Service Model, Opportunity, Security, Maintenance, Prospect of Cloud in Developing Countries.*

I. INTRODUCTION

Cloud computing is a buzzword in the new business model for providing and obtaining IT services that have been established in context of utility computing, grid computing, and autonomic computing a couple of years ago. It aims to provide the clients a cost effective and convenient means to manage the huge amount of IT resources that is actually needed. Today World relies on Cloud computing to store their public as well as personal information. Although cloud computing itself is still not yet mature enough, it is already evident that its most critical flaw in security, many IT companies announce to plan or (suddenly) already have IT products according to the cloud computing paradigm [1]. Many Companies that could be considered as the giant of software industry like Microsoft are joining to develop Cloud services. From a business perspective, this technology is about improving organizational efficiency and reducing cost, often coupled with the objective of achieving a faster time-to-market. From a technology and engineering perspective, Cloud Computing can help to realize or improve scalability, availability, and other non-functional properties of application architectures [2]. The main goal of our paper is to identify, classify, organize and quantify the main security concerns and solutions associated to cloud computing, helping in the task of pin pointing the concerns that remain unanswered.

II. ESSENTIAL CHARACTERISTICS OF CLOUD COMPUTING SYSTEM

Cloud computing is an expression used to describe a variety of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. The National Institute of Standards and Technology's definition of cloud computing identifies "five essential characteristics":

On-demand self-service:. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.
—National Institute of Standards and Technology[3]

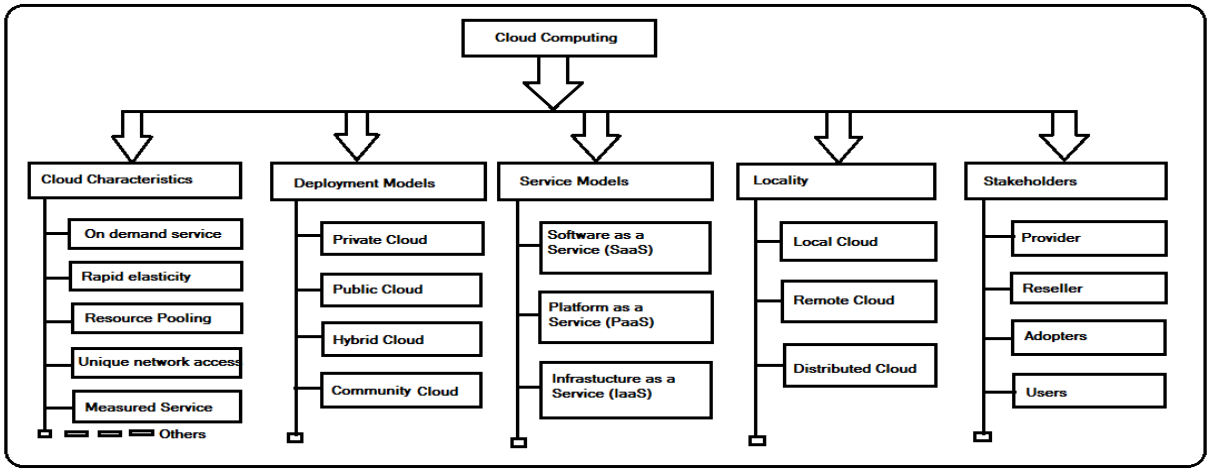

Fig. 2: Non-Exhaustive view on the main aspects forming a Cloud system

III. DEPLOYMENT MODELS

- ***Private Cloud:*** The cloud infrastructure that is managed and operated for one organization only, so that a consistent level of control over security, privacy, and governance can be maintained is called private cloud. It is also known as Internal Cloud or on-premises Cloud. It may be managed by the organization or a third party and may exist on premise or off premise. Its functionalities are not directly exposed to the customer, though in some cases services with cloud enhanced features may be offered – this is similar to (Cloud) Software as a Service (SaaS) from the customer point of view. Example: eBay.
- ***Public Cloud:*** The cloud infrastructure that is made available to the general public or a large industry group and is owned by an organization selling cloud services is called public cloud. It is also known as external cloud or multitenant cloud. Public cloud provide the user with the actual capability to exploit the cloud features for his / her own purposes also allows other enterprises to outsource their services to such cloud providers, thus reducing costs and effort to build up their own infrastructure. As Public Cloud can host individual services as well as collection of services. Example: Amazon, Google Apps, Windows Azure.
- ***Community Cloud:*** The infrastructure which is referred to as special-purpose cloud computing environments shared and managed by a number of related organizations participating in a common domain or vertical market is called community cloud. It may be managed by the organizations or a third party and may exist on premise or off premise.
- ***Hybrid Cloud:*** The cloud infrastructures that is composition of two or more distinct cloud infrastructure (private, community or public) but are bound together by standardized technology that enable data and application portability is called hybrid cloud[4]. It provides benefits of multiple deployment models and enables the enterprise to manage steady-state workload in the private cloud. They will match the economic benefits of global cloud infrastructures with the understanding of local customer needs by providing highly customized, enhanced offerings to local companies (especially SME's) and world class applications in important industry sectors.

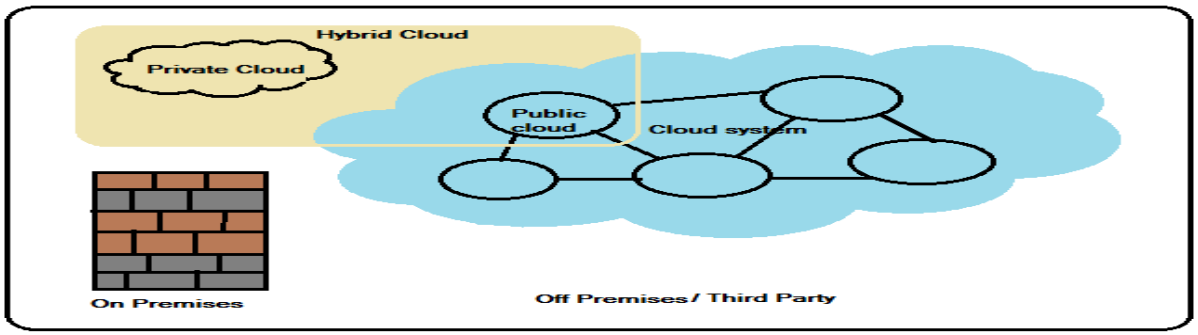

Fig. 3: Presentation of the deployment model of cloud

IV. CLOUD COMPUTING SERVICE MODELS

- ***SaaS (Software as-a-Service):*** The software deployment model, which is the highest form of services that deliver special purpose software to the consumer to use the provider's applications running on a cloud infrastructure through the internet is referred to as Software as-a-Service[5]. It is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis. In the business model using software as a service (SaaS), users are provided access to application software and databases and do not need to manage the cloud infrastructure and platform where the application runs. Cloud providers are responsible for installing and managing the infrastructure and platforms that run the applications. This eliminates the need to install and run the application on the cloud user's own computers, which simplifies maintenance and support. SaaS providers generally price applications using a subscription fee[6]. The main drawback of SaaS is that the users' data are stored on the cloud provider's server. As a result, there could be unauthorized access to the data. For this reason, users are increasingly adopting intelligent third-party key management systems to help secure their data.

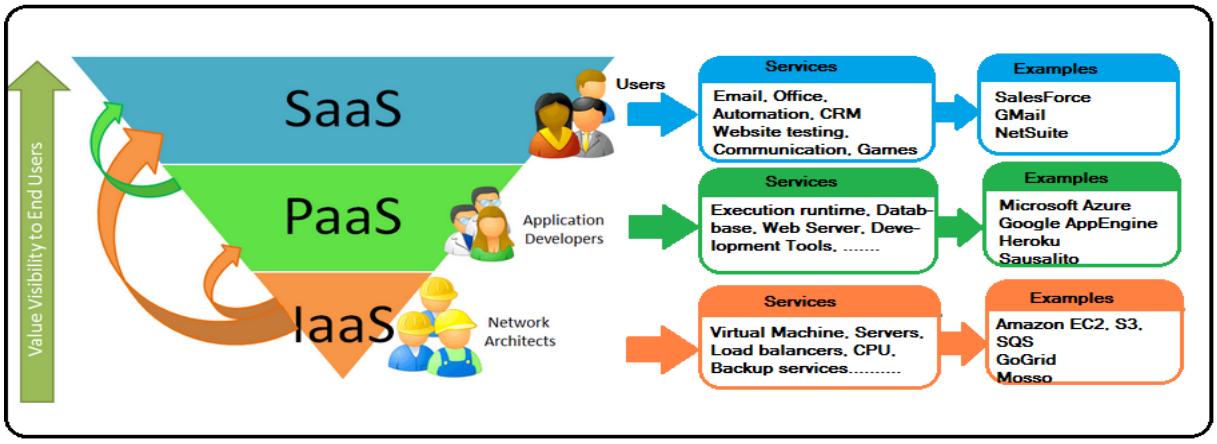

Fig. 4: Presentation of service models of Cloud Computing

- ***PaaS (Platform as-a-service):*** The software deployment model whereby a computing platform is provided as an on-demand service upon which applications can be developed and deployed is referred to as platform as-a-service .It is built on the top of IaaS and joins with software as a service (SaaS) and infrastructure as a service (IaaS), where application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. The development environment is typically special purpose, determined by the cloud provider and tailored to the design and architecture of its platform. The cloud subscriber has control over applications and application environment settings of the platform. Security provisions are split between the cloud provider and the cloud subscriber[7]. There are various types of PaaS vendors; however, all offer application hosting and a deployment environment, along with various integrated services. The table represented below shows some example of PaaS vendor with some of their property:

Platform	**Runtime Environment**	**Service**
Google App Engine	• Java • Phython With restriction	Data storage, Google account Image manipulation, Mail, Memocache etc.
Microsft Azure Platform	Windows Azure, .Net language	SQL Azure, Database, Azure Storage service, Access control etc.
Force.com Salesforce.com	Force.com platform: • Apex (based on Java) • Visualforce(for UI) • Meta Programming	Force.com, Database service, Web service API, Reporting & analytics, Access control, Workflow engine etc.

Table. 1: PaaS vendor with some of their property

- ***IaaS (Infrastructure as-a-Service):*** The software deployment model where the basic computing infrastructure of server, software, and network equipment's are provided as an on-demand service upon which a platform can be developed and execution of applications can be established is referred to as Infrastructure as-a-Service. Its main purpose is to avoid purchasing, housing, and managing the basic hardware and software infrastructure components, and instead obtain those resources as virtualized objects controllable via a service interface[7]. Customers are able to self-provision this infrastructure, using a Web-based graphical user interface that serves as an IT operations management console for the overall environment. The consumer does not need to manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls) and pay only for the resources they use. The table represented below shows some example of IaaS vendor with their property[5]:

Vendor	**Hosting Service**	**Storage Service**
Amazon	Elastic Compute Cloud	Elastic Block Storage(EBS), Simple Storage Service(S3)
ServerPath	GoGrid Cloud Hosting	Go Grid Cloud Storage
Rackspace	Cloud Severs	Cloud Files

Table. 2: IaaS vendor with their property

V. OPPORTUNITIES IN CLOUD

Cloud computing presents an opportunities for both business and social innovation as well as modernizing ICT. Cloud provides a platform for business units to develop and deploy new processes, systems and offerings that make them more competitive. Cloud also helps turn IT into a more effective and responsive business service. Ensuring on-demand access to pools of trusted infrastructure and services, cloud promises to de-couple business initiatives from the IT capabilities driving them. Some of the following issues can be treated as the cloud offers a lots of opportunities to its clients.

- ***Cost efficiency:*** The main objective of cloud computing is to provide the clients a cost-effective convenient means to consume the IT resources in actual amount. As there is no need to install any application in user's computer, cloud also helps to reduce the cost for infrastructure maintenance and acquisition. The visible outward lower barrier is provided by third party mostly and does not need to be purchased for one-time or frequent tasks. Small organization and companies who want to start business with low capital can use open sources cloud computing frameworks. These frameworks are designed to run cloud applications. Some important open source cloud applications are Open Stack, Eucalyptus and Open Nebula **[8]**.

- ***Pay per use:*** The client need to pay only when he use the services and opportunities offered by the cloud. It is strongly related to the quality of service and its support. So it is an option to use the cloud storage rather than using a server costly provided by a company or maintaining by own.

- ***Faster-time to market:*** From a business perspective, the purpose of cloud is to achieve a faster time-to-market. Enterprises such as small and medium want to spread their service to adopt with the growing business competitive with the larger industries. They sell their services quickly and easily with little delays by setting up the infrastructure. Larger enterprises compete the market with greater innovation and less overhead.

- ***Innovation:*** The cloud is creating a foundation for a flexible assembly model to accelerate past tech investment that organization have made and transform them into business model. It also fastening the emerging trend of big data and analytics, mobile computing and social business prior to the innovative ideas. Companies are dealing with these services and linking them to create new and innovative business processes.

- ***Linking inside organization:*** Cloud helps companies to integrate their system to validate the internal operations of a company. Companies manage operations e.g. HR, finance, or warehouse management -to the systems, such as email, social networking or collaboration hubs **[9]**. These services are used to connect with employees, partners and customers. Cloud propel those organizations and companies to make the most productive and the most creative use of data collections.

- ***System automation:*** Larger organizations already control their services and protect their resource and develop privacy rules of their own organizations using the automation of cloud. From the business perspective small and medium organizations also can automate their systems by using cloud services.

- ***Business dimensions:*** Cloud computing technologies drives the business opportunities in a beneficiary ways[10]. It offers various services that leads the organizational business mostly towards rapid growth and nimbleness.
    - ***Growth:*** Whether the business challenge is expanding into new markets, attracting and retaining new customers, executing M&A strategy or speeding up time-to-market for new products and services, cloud allows organizations to rapidly and easily scale up their operations to support business goals.

    - ***Agility:*** The cloud model, with its flexible infrastructures and on-demand pricing, is starting to reset the expectations for IT within business. It presents the opportunity for IT to be re-cast as an enabler of business agility — rather than an inhibitor of business change.

    - ***Adaptability:*** it is an essential features of cloud systems that strongly relate to elastic capabilities. The on-time reaction to changes in the amount of requests and size of resources determine the adaptive capacity of the system of organizations and companies. Adaptation also changes in different environmental conditions such as resources, quality and routes etc.

- ***Green computing:*** Going green is important not only to reduce additional costs of energy consumption, but also to reduce the carbon footprints. It includes the implementation of energy-efficient CPUs, servers and peripherals as well as reduced resource consumption and proper disposal of electronic waste (e-waste). Cloud computing can be mostly an energy-efficient technology for significant energy savings that have so far focused on hardware aspects with respect to system operation and networking sectors. Several cloud service providers now facilitates the green computing[11] options with their services. To reduce the optimal costs annually companies and organizations can focus their services and deals with the thinking "going green".

- ***Recent economic scale:*** Cloud computing continues to gain steam with 56% of the major European technology decision-makers estimate that the cloud is a priority in 2013 and 2014, and the cloud budget may reach 30% of the overall IT budget. According to the TechInsights Report 2013: Cloud Succeeds based on a survey, the cloud implementations generally meets or exceeds expectations across major service models, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). The cloud offers many strong points: infrastructure flexibility, faster deployment of applications

and data, cost control, adaptation of cloud resources to real needs, improved productivity, etc. The early 2010s cloud market is dominated by software and services in SaaS mode and IaaS (infrastructure), especially the private cloud. PaaS and the public cloud are further back **[12].**The promise of cloud is that it can bring together practices, tools, and technologies that will better position a government department to operate in a significantly more efficient, predictable, flexible, and accountable manner. The cloud is not just a technologies anymore.

VI. SECURITY AND PRIVACY IN CLOUD

6.1 SECURITY

Cloud computing has already gained a lot of popularity and is considered the future in the IT industry. The development of cloud service model delivers business supporting technology more efficiently than ever before. Therefore hackers are also interested in it. Various attacks such as social engineering attack, XML signature wrapping attack, malware injection, data manipulation, account hijacking, traffic flooding, and wireless local area network attack pose a great risk to cloud computing systems[13]. There have been many instances where companies have fallen victims to cloud computing being hacked[14].

6.1.1 Types of security: Cloud computing security or, more simply, cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing [15].

6.1.2 Security in different service models: Organizations use the different service models e.g. SaaS, PaaS and IaaS and four deployment models e.g. private, public, hybrid and community cloud. These organizations uses the different advanced security technologies, mostly available because of centralization of data and universal architecture. Cloud itself has the capability to address a number of potential deficiencies of its architecture because of its identity characteristics. But the assumption of this layout architecture may introduce a number of uncategorized threats. We can categorize the threats in cloud computing as the following figure according to the report of Cloud Security Alliance (CSA).

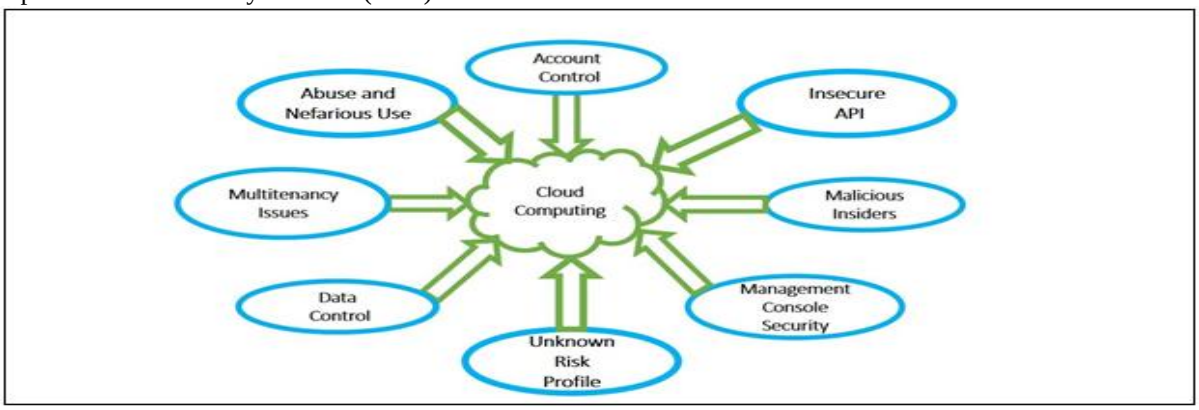

Fig. 5: Categorization of threats in cloud computing

As like as CSA, some other organizations e.g. European Network and Information Security Agency (ENISA) and Information Security Forum (ISF) also added some other security issues in the list of threats of cloud computing. There are also data protection, operational integrity, vulnerability management, business continuity (BC), disaster recovery (DR), and identity management (IAM) make up the list of security issues[16] for cloud computing. Privacy is another key concern — data that the service collects about the user (e.g., event logs) gives the provider valuable marketing information, but can also lead to misuse and violation of privacy.

6.1.3 Security problems and issues: These threats are not listed in any order of severity. The members of both CSA and ENISA ranked the threats to help listing the threats with validation. The listing reflects in the business industries those are using different cloud services. However there ranking indicates that the industries should take participation to initiate necessary steps for the better security. The only threat consistently receiving lower ranking was Unknown Risk Profile, the experts commented that it should be perceived with importance for evaluation and articulation. A figure of the security problems in cloud is depicted here inspired from [17][18].

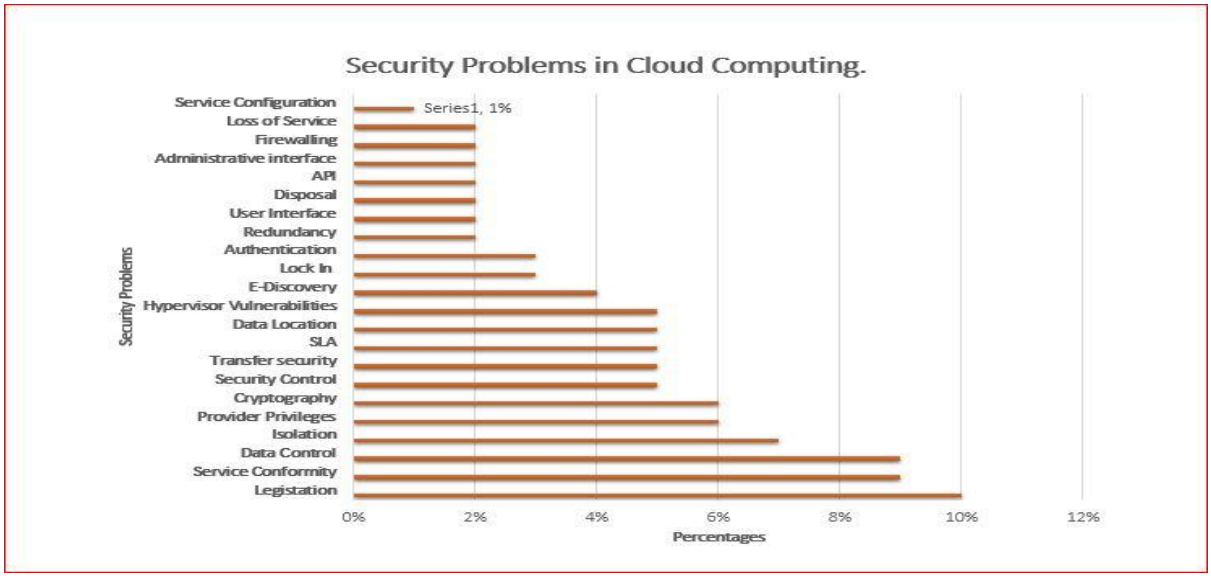

Fig. 6: Security problems in cloud computing.

The results obtained for the number of citations on security issues is shown in Figure (6). The three major problems identified in these references are legal issues, compliance and loss of control over data. These legal- and governance related concerns are followed by the first technical issue, isolation, with 7% of citations. The least cited problem are related to security configuration concerns, loss of service, firewalling and interfaces. Grouping the concerns using the categories presented in section "Cloud computing security"[19] leads to the construction of Figure (7). This figure shows that legal and governance issues represent a clear majority with 73% of concern citations, showing a deep consideration of legal issues such as data location and e-discovery, or governance ones like loss of control over security and data. The technical issue more intensively evaluated (12%) is virtualization, followed by data security, interfaces and network security. Virtualization is one of the main novelties employed by cloud computing in terms of technologies employed, considering virtual infrastructures, scalability and resource sharing, and its related problems represent the first major technical concern [17].

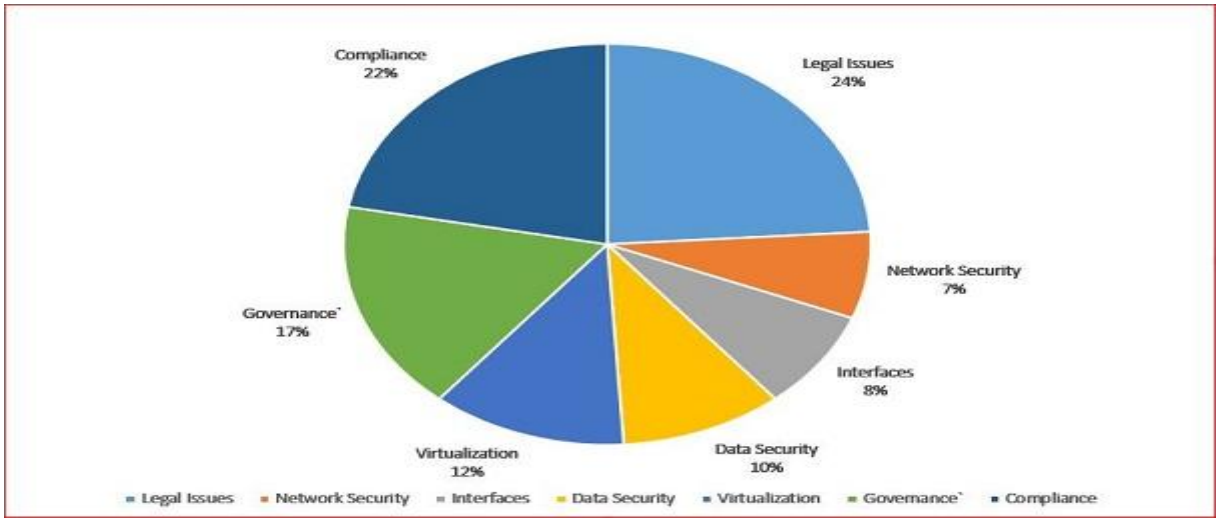

Fig. 7: Security problem with group categories

6.1.4 Security aspect in Virtualization: It is also a major aspect. Virtualization is an essential technology of cloud. It provides flexibility through aggregation, routing, and translation to the user but hides the technological complexity from them. This system is said to be user friendly, infrastructure and location independent and adaptable [20]. There are numerous potential benefits of running workloads with a VM (vs. running them on physical machines). Figure (8) provides an overview of these benefits [21].

Fig. 8: Security benefits of virtualization.

The isolated environments allows VM's system administrators to have the ability to easily configure them in a variety of ways. For example, VM itself can be configured with limited connectivity to the rest of the

environment without the access to the internet and other network. This helps reduce risks related to the infection of a single system. VM can be rolled back to a particular point-in-time during the system violation such as installation of malicious software[22].
Virtualization is often used for performing backups and disaster recovery. Due to the hardware-independence of virtualization solutions, the process of copying or moving workloads can be simplified. In the case of a detected security breach, a virtual machine on one host system can be shut down, and another "standby" VM can be booted on another system. This leaves plenty of time for troubleshooting, while quickly restoring production access to the systems. Finally, with virtualization it's easier to split workloads across multiple operating system boundaries. Due to cost, power, and physical space constraints, developers and systems administrators may be tempted to host multiple components of a complex application on the same computer.

6.1.5 Security solution in VM: Virtual Machine Monitor (VWM) is a software in which the total concept of virtualization implemented. However, current VMMs do not offer perfect isolation. Many vulnerabilities have been found in all virtualization software, which can be exploited by malicious users to gain the access of restricted security privileges [4]. If sensitive data is contained in those VMs, it's often just a matter of time before the data is compromised. Malicious users can also cause significant disruptions in service by changing network addresses, shutting down critical VMs, and performing host-level reconfigurations. Some of the risks are inherent in the architecture itself, while others are issues that can be mitigated through improved systems management. Hardware failures and related issues could potentially affect many different applications and users. In the area of security, it's possible for malware to place a significant load on system resources. Instead of affecting just a single VM, these problems are likely to affect other virtualized workloads on the same computer.

6.2 PRIVACY:

Privacy is another key concern — data that the service collects about the user (e.g., event logs) gives the provider valuable marketing information, but can also lead to misuse and violation of privacy **[15]**. Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted (even better) and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

VII. MAINTENANCE AND MANAGEMENT OF SECURITY IN CLOUD

7.1 MAINTENANCE AND MANAGEMENT OF SECURITY IN GOOGLE CLOUD:

Google manages their security in following ways in their cloud in figure (9). They are Data Center and Network Security, Access and Site Controls, Data, Personnel Security, Sub processor Security [17].

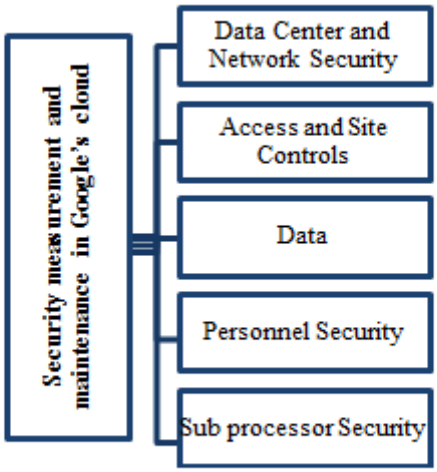

Fig. 9: Security and maintenance in GOOGLE's cloud

In **Data center and network** they maintain the infrastructure of the vast geographic areas and prevents redundancy without interruption according to the internal specification. They uses alternative power backup to provide 24/7 continuous service. They used a Linux based implementation for the customization of the application environment. They process the data storing algorithm to augment data security and redundancy and process code to enhance the security in production environments**.** In the case of **Network and Transmission**, they designed their system to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Google transfers data via Internet standard protocols. They tightly control the size of transmission and make-up of Google's attack surface through preventative measures. It also employs automatic remedy of certain dangerous situations. It monitors a variety of communication channels for security incidents and makes HTTPS encryption (also referred to as SSL or TLS) available **[17]**.

In the case of **Access and Site control**, Google's data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. They maintain formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. The data centers employ an electronic card key and biometric access control system that are linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate.
In **Access Control**, Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Google aims to design its systems to (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. They include password expiry, restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g. credit card data), Google uses hardware tokens.

Google stores **data** in a multi-tenant environment on Google-owned servers. The data and file system architecture are replicated between multiple geographically dispersed data centers. Customer may choose to make use of certain logging capability that Google makes available via the Services. Certain disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving Google's premises either for reuse or destruction.

In **Personnel Security**, Google personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Personnel are provided with security training. Personnel handling customer data are required to complete additional requirements appropriate to their role (e.g. certifications). Google's personnel will not process customer data without authorization.

In Sub Processor Security, prior to onboarding Sub processors, Google conducts an audit of the security and privacy practices of Sub processors to ensure Sub processors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide.

7.2 TRUESTED ISSUES ON THIRD PARTY:

Security issues of cloud computing also relies on third party activities. Third party activities can be trusted upon following reliability issues.

- Low and High level confidentiality.
- Server and Client Authentication.
- Creation of Security Domains.
- Cryptographic Separation of Data.
- Certificate-Based Authorization.

VIII. CLOUD IN DEVELOPING COUNTRIES

The advantages of adopting cloud can be profound for government IT departments, starting with the reduction or redirection of on-site IT staff as well as the ability to access IT resources and infrastructure as needed. The importance of having a cloud computing strategy is becoming more obvious on a daily basis. A lot of companies is moving towards this interesting technology. Different organizations and companies from different countries already showed their significant capabilities at the growing business of cloud computing. The growth is based on real business opportunities[23]. Economically some developing countries also become inclined to the cloud computing technologies. Cloud offers these countries some of its features at low cost and provides more flexibility than previous. For a growing number of organizations worldwide, cloud computing offers a quick and affordable way to tap into IT infrastructure as an Internet service. But obstacles and challenges remain.

8.1 OVERALL STATISTICS OF DATA STORAGE IN CLOUD SERVER:

The desire to share content and to access it on multiple devices will motivate consumers to start storing a third of their digital content in the cloud by 2016, according to Gartner, Inc. Gartner said that just 7 percent of consumer content was stored in the cloud in 2011, but this will grow to 36 percent in 2016 **[24]**. Annual global data center IP traffic will reach 8.6 Zettabytes (715 Exabyte [EB] per month) by the end of 2018, up from 3.1 Zettabytes (ZB) per year (255 EB per month) in 2013. Global data center IP traffic will nearly triple (2.8-fold) over the next 5 years. Overall, data center IP traffic will grow at a compound annual growth rate (CAGR) of 23 percent from 2013 to 2018 **[25]**. The growth of the distribution of cloud traffic significantly increases every years. The distributed cloud traffic map of 2012 is pictured below **[26]**.

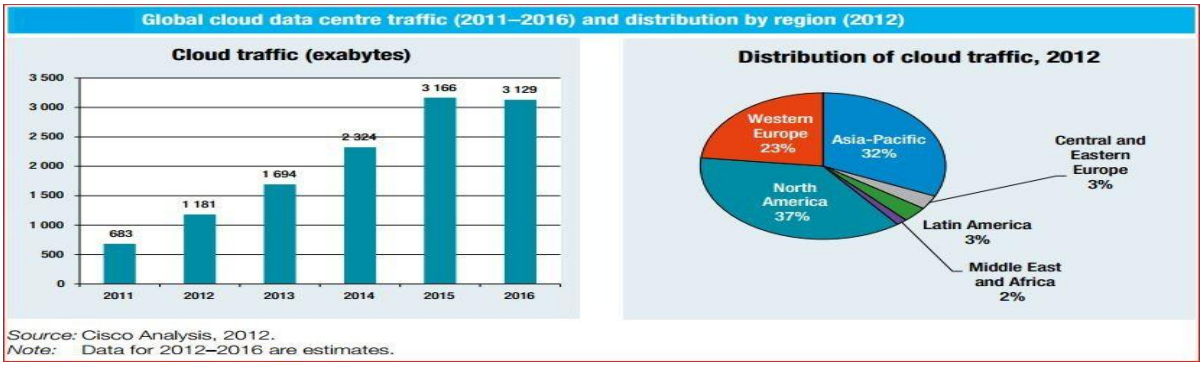

Fig. 10: Distribution of cloud traffic of the world

Most of these data are from the developed countries like Japan, Australia[27], US, Germany, Singapore, France, UK, Korean, Canada, Italy, Spain, Poland, Malaysia, Russia, Mexico, Argentina, India, Turkey, China, Indonesia, Brazil and some other big large countries.

8.2 CURRENT SITUATION IN DEVELOPING COUNTRIES:

Developed and large countries manage large amount of data while other countries of the 3rd world really fall backwards than those developed countries. In fact many of the countries did not set up cloud computing servers because of either lack of proficiencies in the management and operating of servers or lack of capacities to bear the cost. For example According to the "Information Economy Report 2013 [26]", 28 percent of internet users in the developed countries had taken broadband services in 2012. The rate, however, was a mere 0.3 percent in Bangladesh. On the other hand, 0.5 percent internet consumers use mobile broadband services in Bangladesh. The rate is 67 percent in the developed nations [26]. According to the UN report, a lack of access to affordable broadband and data servers in developing countries severely limits the scope of 'cloud computing' that uses vast, shared virtual servers instead of localized hardware to run applications and store data. In June 2013, more than 60 percent of located IXPs are form Europe and North America. In Africa, which was home to only 6 percent of the world's IXPs. Distribution of co-location data centers, by group, 2013 shows the Co-location data centers for developing economies consumes 85% of storage in the data centers while only 13% of storage remain for the developing countries. Least developed countries consumes no storage in the cloud [26].

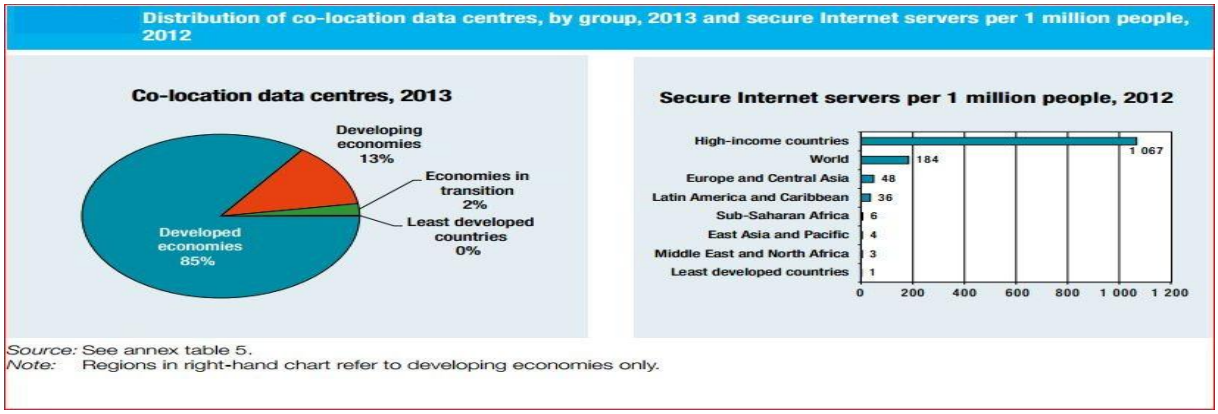

Fig. 11: Distribution of co-location data centers, by group, 2013

IX. OFFERS FOR DEVELOPING COUNTRIES

Cloud computing and cloud services offers potential advantages to the customers. As the cloud computing ecosystem evolves, the organizations and companies from the developing world should consider these offers **[26]**. These potential offers are the great opportunities for the developing nations to grow their business in a significant manner. These offers include:

- Reduced costs for rented IT hardware and software compared to in-house equipment and IT management.
- Enhanced elasticity of storage/processing capacity as required by demand.
- Greater flexibility and mobility of access to data and services.
- Immediate and cost-free upgrading of software.
- Enhanced reliability/security of data management and services.

X. OBSTACLES

Also cloud offers several benefits to the developing nations, there are some potential risk which are considered as the obstacle to spread the services of cloud**.** These obstacles include:

- Increased costs of communications (to telecommunication operators/Internet service providers (ISPs)).
- Increased costs for migration and integration.
- Reduced control over data and applications.
- Data security and privacy concerns.
- Risk of services being inaccessible, for example, due to inadequate ICT or power infrastructure. Risk of lock-in (limited interoperability and data portability) with providers in uncompetitive cloud markets.

XI. EXPECTATION

The progress of cloud computing creates the opportunity for entrepreneurs, small and large business, researchers, and governments. For the developing countries e.g. Bangladesh, Sri-Lanka, Nepal, Bhutan in ASIA and developing countries in AFRICA, it is a potential level of playing field because cloud computing offers an opportunity to create entirely new types of business and models that couldn't have been imagined or beyond possibilities few years ago. Most of the developing countries have lacking of dedicated servers for storing important and secure data. In this case cloud store offers them the storing places with low costs or entirely for free. The expectance of developing countries is to grow their business with highest possible security and nimbleness. The functions of cloud computing would be applied towards development listed as e-education, e-health, e-commerce, e-governance, e-environment, and telecommuting. These functions are areas that governments and aid agencies can devote projects and resources to in order to improve a target socio-economic statistic in developing countries.

XII. CONCLUSION

Currently Cloud Computing is an emerging discipline that helps the IT industries to get efficient use of their Hardware and Software resources and enabling service-oriented, on-demand network access to rapidly scalable resources with promises to cut operational and capital cost. For developing countries, cloud computing can be an appealing vision for cheap communications. But with advancement of cloud technologies and the increasing number of cloud users, data security dimensions are continuously increasing. As todays cloud computing technologies are vulnerable to security attacks, so for security-sensitive applications of a Cloud computing requires high degree of security and maintenances. So we think, the major problems of cloud need to be resolved before major users will adopt clouds for sensitive data and computations. In this paper, we have discussed and analyzed cloud computing environment to clarify the opportunity of current cloud technology for developing countries with its data security risks, vulnerabilities and some possible solutions. We immensely hope that our paper will be useful to researchers currently working and people who are feeling interest in advancement of cloud computing technology.

REFERENCES

[1] Vikas Kumar, Swetha M.S, Muneshwara M. S., Prof Prakash S,CLOUD COMPUTING: TOWARDS CASE STUDY OF DATA SECURITY MECHANISM, International Journal of Advanced Technology & Engineering Research (IJATER).

[2] Dimpi Rani , Rajiv Kumar Ranjan, A Comparative Study of SaaS, PaaS and IaaS in Cloud Computing, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6, June 2014, ISSN: 2277 128X

[3] "The NIST Definition of Cloud Computing". National Institute of Standards and Technology. Retrieved 24 July 201

[4] Rajesh Piplode, Umesh Kumar Singh, An Overview and Study of Security Issues & Challenges in Cloud Computing, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, September 2012, ISSN: 2277 128X

[5] Prof. Dr. Andreas Polze, A Comparative Analysis of Cloud Computing Environments, available at : http://drngpasclibrary.pbworks.com/f/cloud-study.2.pdf.

[6] Cloud Computing: http://en.wikipedia.org/wiki/Cloud_computing

[7] Security in Cloud: http://blogs.forrester.com/security_and_risk/2009/11/cloud-security-front-and-center.html

[8] Jisha S. Manjaly, Jisha S, A COMPARATIVE STUDY ON OPEN SOURCE CLOUD COMPUTING FRAMEWORKS, International Journal of Engineering and Computer Science ISSN: 2319-7242, Volume 2, Issue 6 June, 2013 Page No. 2026-2029

[9] Rapid Innovation of Cloud: http://www.forbes.com/sites/ibm/2014/09/02/three-ways-cloud-computing-is-driving-rapid-innovation/

[10] Cloud Computing Issue: http://en.wikipedia.org/wiki/Cloud_computing_issues

[11] Monica B. Harjani*, Dr Samir M. Gopalan**, Comparative study between Green Cloud Computing and Mobile Cloud Computing, International Journal of Scientific and Research Publications, Volume 3, Issue 3, March 2013, ISSN 2250-3153

[12] GEORGE FEUERLICHT1,2 AND NIKOS MARGARIS2, Cloud Computing Adoption: A comparative study ,Available at: www.cssi.cz/cssi/system/files/all/2012_12_07_seminer_Feuerlicht.pdf

[13] S. Gajek, M. Jensen, L. Lioa and J. Schneck, Analysis of signature wrapping attacks and countermeasures, IEEE International Conference on Web Services, 2009.

[14] Michael Hauck, Matthias Huber, Markus Klems, Samuel Kounev,J¨ orn M¨ uller-Quade, Alexander Pretschner, Ralf Reussner, Stefan Tai, Challenges and Opportunities of Cloud Computing, Karlsruhe Institute of Technology, Technical Report, Vol. 2010-19.

[15] Cloud Computing Security: http://en.wikipedia.org/wiki/Cloud_computing_security

[16] Security of Cloud Computing Providers Study, Sponsored by CA Technologies Independently conducted by Ponemon Institute LLC Publication Date: April 2011 .

[17] Cloud Data Processing Terms: https://cloud.google.com/terms/data-processing-terms

[18] Chimere Barron, Huiming Yu and Justin Zhan, Cloud Computing Security Case Studies and Research, Proceedings of the World Congress on Engineering 2013 Vol II, WCE 2013, July 3 - 5, 2013, London, U.K.

[19] Jaliya Ekanayake 1,2, Xiaohong Qiu1, Thilina Gunarathne1,2, Scott Beason1, Geoffrey Fox1,2, High Performance Parallel Computing with Cloud and Cloud Technologies , available at: http://cgl.soic.indiana.edu/publications/cloudcomp_camera_ready.pdf.

[20] Nelson Gonzalez1*, Charles Miers1,4, Fernando Red´ ıgolo1, Marcos Simpl´ıcio1, Tereza Carvalho1,Mats N¨ aslund2 and Makan Pourzandi3, A quantitative analysis of current security concerns and solutions for cloud computing, Gonzalez et al. Journal of Cloud Computing: Advances, Systems and Applications 2012, 1:11 http://www.journalofcloudcomputing.com/content/1/1/11

[21] Virtualization in Cloud: http://anildesai.net/index.php/2007/05/virtualization-security-pros-and-cons/

[22] S. Qaisar and K. Khawaja, Cloud computing: network/security threats and countermeasures, Interdisplinary Journal of Contemporary Research In Business Volume 3, January 2012.

[23] Coud Computing Adoption in Developing Countries: http://cloudtweaks.com/2014/06/cloud-computing-adoption-developing-countries/

[24] http://www.gartner.com/newsroom/id/2060215 , Press Release, STAMFORD, conn, June 25, 2012.

[25] *Coud Index White Paper:* http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html

[26] "Information Economy Report 2013", The Cloud Economy and Developing Countries", "UNCTAD/IER/2013, Sales No. E.13.II.D.6, ISSN 2075-4396, ISBN 978-92-1-112869-7, e-ISBN 978-92-1-054154-1

[27] *The Cloud Score card:* http://cloudscorecard.bsa.org/2013/