DOI : https://doi.org/10.56452/7-12-34

ISSN: 0974-5823 Vol. 7 No. 12 December, 2022

International Journal of Mechanical Engineering

DISCUSSING THE CHALLENGES AND FUTURE TRENDS OF CLOUD COMPUTING

Dibyendu Mahato, Dr. Ajay Jain

Department of Computer Application, Dr. A.P.J. Abdul Kalam University, Indore (M.P.), India

ABSTRACT

As a form of internet-based computing, "cloud computing" delivers services via the internet and, on demand, draws on the user company's internal resources stored in its "private-own cloud" or a remote server. The model is distinguished by its three distinguishing features: scalability, pay-per-use, and self-services. In the wake of rising demand for online services and utility computing, "the cloud" has emerged as a focal point in the modern era of information technology. One of the most difficult aspects of offering robust processing and storage as on-demand services is the security risk coming from resource sharing over the cloud. The study delves into the difficulties and emerging tendencies of cloud computing.

Keywords: Cloud computing, Security, Service Providers, Challenges

I. INTRODUCTION

In cloud computing, a "cloud" refers to a collection of networks, just as in the real world, clouds are a collection of water droplets. The user has unrestricted access to cloud computing's capabilities at any time they're needed. Users often choose an intermediary provider for the service of the internet in cloud computing rather than building up their own physical infrastructure. Only the time actually spent using the service is charged to the user. In cloud computing, the workload can be moved to another server. The networks that make up the cloud carry the most of the service demand, thus executing an application locally does not tax the system too much. As a result, less user-side hardware and software is required. To access cloud services, all we need is a computer with an internet browser. To access cloud services, only a web browser, such as Chrome, is required. Cloud computing is an evolution of grid computing, distributed computing, and parallel computing in which all resources are made available to users on demand. It's a blueprint for making flexible IT assets available. Therefore, cloud computing can be defined as the provision of an Internet-based computing service that allows for convenient, on-demand network access to a shared pool of resources. Cloud computing expands on established methods of data processing including grid computing and virtualization. These are the many distributed computing models. Data, processing, and applications are typically assigned to remote servers in cloud computing. Computing resources like as servers, storage, networks, applications, and services are pooled and made available to users on demand under this paradigm. Users and businesses alike may take use of a wide range of features offered by cloud computing and storage solutions by storing and processing their data at remote data centers. In order to achieve network-wide consistency and expand economically, resource sharing is essential. Cloud computing is in

DOI : https://doi.org/10.56452/7-12-34

high demand because of its many useful features. These features include low service costs, high performance and processing power, scalability, accessibility, and availability.

The use of cloud computing is a trend that is rapidly gaining popularity throughout the globe. The term "cloud computing" refers to a system that allows users to access programs that are housed in off-site data centers. Cloud computing may be understood as a remote data center. It provides the Infrastructure, Platforms, and Software on a pay-for-use basis and acts as a facilitator for the pooling of technological resources, applications, and digital content over the internet. Information and resources may be stored and accessible from anywhere in the world at any time. User benefits from cloud computing include scalability, access to specialized processing resources, reduced workload, and lower capital costs. While cloud computing has many benefits, it also presents some difficulties.

The services provided by the cloud may be broken down into three broad groups. Software-as-a-service (SAAS) is the first form of cloud service. Access to the service provider's software applications hosted in the cloud is made possible by this service. The application is managed and controlled by the service providers. Customers can pay to access the API online rather than buying the product outright. Google Docs, for instance, uses JAVA Script, a language that can be executed in a web browser.

The second category of cloud service is known as "Platform as a service" (PaaS). It's yet another method for getting programs to users. By utilizing the provider's cloud infrastructure and the languages and tools provided by the provider, users may easily install their own apps. While the cloud provider is responsible for the underlying infrastructure, the end user is in charge of the software being used. The Google App Engine is a service that allows programmers to create applications that can then be deployed on Google's servers.

Last but not least, there's Infrastructure-as-a-service (IaaS) cloud computing. This service simply provides developers with virtual machine images as a service, and the VMs may be loaded with anything they choose. Customers can obtain the services of servers, software, data center resources, network equipment, and the personnel who know how to run it all as an outsourced service provided via the network cloud. The number of active virtual machines can be dynamically adjusted by the user to meet their changing needs. Instance-level firewalls, for instance.

II. HISTORY OF CLOUD COMPUTING

In the 1950s, the concept of large-scale shared infrastructure, such as mainframe computers, was initially proposed. It enables users to work effectively and utilize many terminals at once. But it wasn't until the last 10 or so years that cloud computing truly started to develop into the monstrosity we know it to be today. If you were seeking to buy servers ten or twenty-two years ago, you probably remember how expensive the actual hardware was, even if it wasn't as expensive as mainframes from the 1950s. The prices had to decrease significantly as more people expressed a want to be online, and virtualization was one of the strategies that made this possible. Servers were virtualized into shared hosting environments, Virtual Private Servers, and Virtual Dedicated Servers using the same functionalities that the VM OS provided in the 1950s. If your company required 13 physical systems to power its websites and software, it would be an example of how that really worked in practice. By using virtualization, these 13 separate systems may be divided across two physical nodes. Naturally, in this sort of environment, you would need less physical hardware to meet the needs of your business, which would result in cheaper infrastructure costs. It is possible to realize, modernize, update, compound, and further develop many of the given technologies,

DOI : https://doi.org/10.56452/7-12-34

results, and ideas in tandem with the creation of objective requirements (hardware and software).

By first renting out its datacenter to outside customers for personal use, Amazon played a significant role in the development of cloud computing. In 2006, they released the utility computing platform Amazon EC2 and S3.

A number of important companies followed suit, releasing one after another cloud-based solutions, including IBM, Google, HP, Sun, Forces.com, Microsoft, Yahoo, and others.

Since 2007, the number of trademarks covering cloud computing companies, goods, and services has increased at a nearly exponential rate.

The Academic Cloud Computing Initiative (ACCI), a research project aiming at addressing the challenges of large-scale distributed computing, was founded in 2007 by Google, IBM, and a number of universities. In addition, cloud computing is a very well-liked research topic.

Since 2008, a large number of open-source projects have consistently appeared. For instance, Eucalyptus is the first API-compatible platform for building private clouds. Open Nebula, which also offers private and hybrid clouds, federates many cloud modes.

HP announced Site on Mobile in July 2010 for developing regions where people are more likely to access the internet through mobile devices than PCs. With more and more individuals owning smartphones, mobile cloud computing has become more and more popular. Several mobile network providers, including Orange, Vodafone, and Verizon, now provide cloud computing services for enterprises.

In March 2011, Deutsche Telecom, Facebook, Google, Microsoft, Verizon, and Yahoo founded the Open Networking Foundation, a grouping of 23 IT companies. This NGO is supporting Software- Defined Networking, a recent cloud initiative. The program's objective is to use small software changes to speed up innovation in data centres, wireless networks, telecommunications networks, and other networking areas.

III. FEATURES OF CLOUD COMPUTING

Cloud computing offers a wide range of benefits, including the following.

Individual Service on Request

The user may access the online resources whenever he or she wants, without having to communicate with each individual server. Time on a server, data space on a network, programs, etc., all fall under this category. A user with an urgent need at a certain moment may thereby use these computational resources in a timely fashion, without the requirement for any human contacts with the providers of these services.

Network Access on Wide Range

Access to the network's resources is possible through a wide variety of thick and thin client devices, including smartphones, laptops, tablets, desktop computers, and more. The internet makes all of these materials readily available to anybody who wants to utilize them.

Distribution of Resources

In order to accommodate several users, the available online computer resources are pooled together. A multitenant paradigm is implemented, and various types of virtual and physical resources are allocated and reallocated as needed. Although the user may be able to determine the location of resources at a more advanced level of system customization, such as storage, data processing, memory, and network bandwidth, the distribution of resources is

DOI : https://doi.org/10.56452/7-12-34

an independent process in which the user has no influence over the physical parameters of the resources. Cloud computing makes advantage of the multi-tenancy virtualization concept to pool resources for the benefit of several customers. The motivations for the cloud computing system are economies of scale and specialization.

Efficient Elasticity

In cloud computing, answers to issues may be found quickly and easily whenever they are needed. Because solutions are linked to both incoming and outgoing demand, resources may be readily allocated and released automatically. As the server's workload increases, any bugs or restrictions imposed by the hardware or software are fixed or adjusted as necessary. It would appear that the users had access to an infinite supply of resources that can meet their every conceivable need.

Evaluated service

The cloud system automatically optimizes and regulates services including processing, storage, user accounts, bandwidth, etc. At some level of abstraction, these services are also rated in accordance with user needs. In Cloud Computing, the services used by the user are easily managed, tracked, and reported on with pinpoint accuracy for both the consumer and the service provider.

Self-Curing

When an application fails, cloud computing is able to give a "baking copy" that is already set up and ready to record the error without causing any disruptions. Multiple, up-to-date copies of each program are kept in the event of a crash; this ensures that the remaining applications can continue to operate normally.

Multi-tenancy

Multi-tenancy in the cloud refers to the simultaneous use of several tenants in a same application. Many users in this system share the same hardware, yet almost none is aware of this fact. The server may be made available to multiple users by vitalizing the machine pool. Users may be assured that their information is safe and secure during this procedure.

Linearly Scalable

In cloud computing, services may be expanded in a linear fashion. This system partitions the workload and distributes it to other nodes in the network. For instance, if a single server can handle one thousand transactions per second, then two servers may handle two thousand transactions per second, illustrating the linear scalability of the system.

Service oriented system

Cloud computing is a service-oriented architecture, meaning that it is built from smaller components called "services." In order to make better use of the existing and future Cloud Computing services, it is common practice to combine many separate offerings into a single service.

Service Level Agreement

Cloud computing relies on service level agreements (SLA) to handle peak server loads. Adjustments to the load are made automatically so that SLAs may be met. Whenever the services need to handle a larger workload, they simply spin up more instances of the application on separate servers.

DOI : https://doi.org/10.56452/7-12-34

Virtualized

on cloud computing, each program runs on its own separate virtual machine, disconnected from the host computer and its surrounding environment. This separation ensures that the failure of one virtual machine does not disrupt the operations of the others, and that data is not exchanged between them.

Stretchable

The flexibility of cloud computing services allows them to be utilized for a wide range of workloads, from light consumer applications to heavy enterprise workloads.

IV. CLOUD COMPUTING APPLICATIONS

The potential uses of cloud computing are many. It is possible to execute nearly any program on a cloud computing system by installing the appropriate middleware.

- Customers may get to their files and programs from any Internet-connected device, whenever and whenever they choose.
- Historically, businesses that rely heavily on computers have had to purchase software licenses for each employee. Using a cloud computing system, these businesses can gain access to all the necessary software without having to purchase the software themselves. The business can instead contract with a cloud service provider on a pay-as-you-go basis.
- There will be less need for expensive client hardware thanks to the cloud computing architecture. The user can avoid spending extra money on a supercomputer with a huge hard drive just to store his data. This customer's requirement will be met through a cloud-based service. The client need only acquire a terminal with a display and input devices powered by only enough computing resources to execute the middleware required to link to the cloud system.
- Servers and other forms of digital storage need a lot of physical space in most businesses. Because they don't have enough room at their headquarters, some businesses have to rent off-site facilities just to house their data centers' servers and databases. By using a cloud computing system, businesses are able to store their data on the servers of third parties (cloud service providers), eliminating the need for costly and space-consuming on-premises data centers.
- Clients have access to the vast computing resources of the cloud. Similar to grid computing, clients can offload extremely computationally intensive tasks to the cloud. It can take a single computer year to complete very complicated computations. In this scenario, the cloud system will utilize the processing capacity of the necessary number of back-end computers to expedite the computation.

V. STANDARDS FOR SECURITY IN CLOUD COMPUTING

Standards for security outline the steps to take in order to put in place a comprehensive security strategy. Information technology (IT) tasks that include the cloud are subject to the same guidelines, which detail the measures that must be done to guarantee the privacy and safety of sensitive data in the cloud. The foundational ideas of security standards are geared toward safeguarding this sort of reliable setting. Defense in depth is a core tenet of security based on the idea of many levels of protection. To ensure safety in the event of a system failure, it is necessary to employ redundant safeguards. Combining a firewall and an intrusion detection system (IDS) is a good illustration of this concept. With defense in depth, attacks are thwarted because they cannot focus their efforts on a single-entry point or weak spot. Therefore, it is a false dichotomy to say that network security can only be implemented at the network's endpoints or in the cloud. Rather of focusing on securing just one system, it is preferable to secure everything. Layered security like this is exactly what's evolving on the cloud. Endpoints, or the points of interaction between a user and a system, have historically been the focus of security measures. There was no way to protect a company's internal network without installing firewalls, intrusion detection systems, and antivirus programs. Extra protection for data stored in the cloud is now feasible thanks to the emergence of managed security services provided by cloud vendors.

Security Assertion Markup Language (SAML)

When it comes to sharing credentials and other data between networks, SAML is the gold standard. Businesses can safely communicate with one another by exchanging identification and entitlement statements. The Security Assertion Markup Language (SAML) standardizes the usage of XML for both requests and answers relating to user authentication, entitlements, and attributes. This format may then be used to query a SAML authority for a principal's security credentials. One platform or app that can communicate security information is a SMAL authority, also known as the asserting party. A partner site that gets the security data is the relying party, assertion consumer, or asking party. Authentication, authorisation, and topic attributes are all part of the data that is sent around. A person with an email account or a printer with a paper jam are both examples of subjects inside their respective domains. SAML is based on several other standards, including Simple Object Access Protocol (SOAP), Hypertext Transfer Protocol (HTTP), and XML. SAML requires the usage of HTTP and SOAP as its communication mechanism.

Open Authentication (OAuth)

Open authorization (OAuth) is an open protocol created by Blaine Cook and Chris Messina that provides a standardized and easy way for web apps of all kinds to implement secure API authorization. OAuth is a protocol for allowing public access to and manipulation of private information. OAuth is a protocol that helps developers safeguards their users' accounts while still granting them access to their users' data. Users can exchange data with both the service provider and their other customers without revealing too much personal information. OAuth serves as a foundation upon which additional protocols and features may be built. OAuth Core 1.0 is lacking in several desirable capabilities due to its architecture. These include automatic endpoint discovery, language support, support for XML-RPC and SOAP, a standardized definition of resource access, OpenID integration, signature methods, etc. The protocol's core focuses on its most essential features, such as the means by which a username and password may be traded for a token with certain permissions, and the means by which that token can be secured. Understand that the protocol does not ensure your security or privacy. In reality, OAuth cannot guarantee confidentiality without relying on additional protocols like SSL.

OpenID

It is a public, distributed protocol for identifying users and determining their permissions. With it, a single digital identity may be used to access a wide variety of online resources. It's an SSO (single sign-on) authentication system. By using OpenID, users just need to remember a single set of credentials that will grant them access to a wide variety of systems. An OpenID is a custom URL that is validated by the organization that is also hosting the user's data. Users' identities need not be verified by an external party thanks to the OpenID protocol. Websites that request identification over the OpenID protocol have no authority to insist on a particular authentication method, and therefore users are free to use any method they choose, including smart cards, biometrics, or plain old passwords.

SSL/TLS

When it comes to protecting sensitive information during transmission over TCP/IP, cryptographically secure protocols like Transport Layer Security (TLS) and its precursor Secure Sockets Layer (SSL) are your best bet. Both TLS and SSL encrypt the transport layer of network communications. TLS is a protocol for secure client-server communication across insecure networks, with the goal of preventing eavesdropping, message forging, and manipulation. TLS employs encryption to offer endpoint authentication and data secrecy. Since the client already knows the server's identity, TLS authentication only works in one direction, authenticating the server. The client is still not verified in this scenario.

VI. CLOUD COMPUTING CHALLENGES

In the preceding paragraphs, we mentioned some advantages of cloud computing. When data is inaccessible to users, however, it is neither an optimal solution nor risk-free. Since users are wholly reliant on cloud resources, there are also concerns about reliability and system performance when making the transition to the cloud. For instance, customers may be concerned about the round-trip time (RTT) required to carry out the operation while connecting to the cloud in order to look for a service. If the cloud is already busy with other instances or if there is heavy traffic, this might be made worse. Users often find it difficult to trust cloud services due to privacy and security concerns. The following are examples of some of the most serious problems associated with cloud computing:

Reliability

The availability and security of the underlying application infrastructure must be assured by a cloud computing service. When dealing with a system on a grand scale, it's imperative to find a reliable solution. Additionally, a dynamic network management system regulates the efficiency and health of the resource nodes by dynamically migrating inefficient or broken nodes. Therefore, these nodes do not have an effect on the overall performance of the system. Keeping everything in the cloud running smoothly and reliably is a never-ending battle.

Resource Provisioning and Scheduling

New difficulties arise for management systems and cloud platforms due to the dynamic deprecation and augmentation of resources based on user demand. An efficient cloud resource provisioning method that improves resource usage and allocation, lessens reaction time, and is both resilient and fault tolerant is urgently needed. As with long-term resource reservation, scheduling for on-demand resource needs can be difficult if there are a large number of resources and users.

Management Issues

Managing a cloud computing infrastructure is a challenging task. In particular, research on resource consolidation has flourished in recent years, making it one of the most important fields of study. It includes taking care of the clients, their billing systems, and service agreements, as well as managing the methods of regulating the system's resources effectively. However, there are drawbacks to using a single service provider. These include (i) the high energy consumption required to keep a massive data center online; (ii) the vulnerability of centralized cloud data centers to multiple points of failure; and (iii) the need to physically

DOI : https://doi.org/10.56452/7-12-34

move data from its original location to the data center for processing. This means that any private or sensitive information created by a program is stored somewhere other than the program itself.

Fault Tolerance

Fault tolerance is the ability of cloud services to keep running regardless of whether or not there is a problem with the hardware or software. Maintaining full system functionality and performance in the face of a problem in such components is a formidable issue.

Privacy and Transparency

Any cloud computing system must adhere to strict standards of data privacy and service transparency. Since users' information and associated credentials are stored in the cloud, protecting that information is essential to earning users' confidence in the service. The same holds true for the virtualization of all systems and infrastructure and the availability of cloud services. Cloud service providers have a responsibility to educate their clients on the handling, storage, and transmission of their data. From the perspective of a customer, especially a large business, it is crucial to know what kinds of security and privacy schemes are in place, as well as what kinds of internal rules and technology are in use.

Security

One of the major problems with cloud computing is keeping data secure. It addresses problems with data security, information security, data integrity, and data confidentiality of all types. When it comes to putting trust in the cloud, security is one of the biggest questions. Therefore, it is essential to this work that it and the related issues be thoroughly discussed.

VII. FUTURE TRENDS IN CLOUD COMPUTING

The whole information technology sector will eventually adopt a strategy called automation, but that's still five years away. Within the next five years, AI and ML will likely become pivotal components of the automation process. Traditional programming employment in the IT sector are expected to decline as automation advances.

Let's make up a scenario to help illustrate the above discussion. We can foresee the INTRUSION that will occur as a result of automation, when a machine rather than a human brain constructs the reasoning. It takes a reasonable length of time for a conventional programmer to complete an assignment by making full use of the computer's capabilities by employing his or her knowledge and expertise. In contrast, the identical task may be completed in a matter of seconds by a machine equipped with the latest technology and the intelligence it gained via machine learning. The conventional IDS systems would be inappropriate in this automated setting. For this reason, it is crucial to immediately fortify conventional security methods like FIREWALLS and IDS.

Only 1% of the world's devices are connected to the internet and making use of cloud services in 2016, according to the report Cyber Security: Threats, Reports, and Challenges. By 2023, analysts predict that 85 percent of global gadgets and industries would choose the internet and cloud as their primary source of service. As the number of connected devices grows, so does the strain on cloud infrastructure. This also leads to a rise in security concerns that are beyond the scope of currently available solutions. New research is needed into how to fortify the cloud, and improvements in security measures are urgently needed. How can we ensure the safety of our facilities? That way, we can keep a firm grasp on things even if a modern cyberattack targets one of our automated systems or services.

Cloud computing's commercial viability has contributed significantly to the rising carbon emission from ICTs, calling into doubt the technology's claimed energy efficiency and eco-friendliness. Carbon emissions are expected to increase from their current level of 7.8 billion tons per year by 2020, a rate that would quadruple the rate of increase seen between 2002 and 2010. While several studies have shown that cloud computing is a Green Technology, others have shown that the widespread use of cloud computing and the associated growth in the number of data centers is causing an alarming rise in atmospheric CO2. Cloud computing has numerous Green qualities thanks to the Cloud framework, however to realize these benefits, more technological initiatives are needed. Following is a list of some:

- System energy economy may be improved by careful software design at several levels (compiler, algorithm, operating system, and applications). Allocating resources to an application based on its performance needs helps keep energy and consumption tradeoffs stable.
- In order to reach the highest possible degree of efficiency in green cloud computing, cloud providers must first evaluate and measure the current data center power, the power consumptions of servers, their cooling demand, and their cooling designs. In addition, modeling tools for the cloud are needed to quantify the energy consumed by its many parts and services.
- Data center resource scheduling designs that don't take into account aspects like network, memory, cooling, and CPU are likely to fail.
- To ensure that the health of human society is not jeopardized by the changes brought about by evolving technology, it is the social obligation of both consumers and providers to ensure that this does not occur. To make the most of Green energy, cloud companies should place data centers in close proximity to renewable power plants.
- To achieve the most advantage in terms of energy efficiency, new technologies like virtualization should be included only after a thorough study of overhead has been conducted.
- If a cloud service is serious about reducing its environmental impact, it has to take steps to increase its use of renewable energy sources and lower its electricity use.

VIII. CONCLUSION

Recent years have seen a surge in interest in cloud computing from both industry and academia, reflecting its status as a key component of the advanced civilizations of the future. Cloud computing's enabling properties are of interest to governments, organizations, and businesses. Nowadays, with the advancement of technology, there has been a growth in assaults, making it increasingly difficult to safeguard your data via a network and the internet without a security control to protect your data from numerous attacks. Security concerns in the cloud are the most pressing. Concrete criteria for the safety of cloud computing can be defined in the future. Cloud data storage and retrieval may be made more secure with the use of cutting-edge encryption methods. To further ensure that only authorized parties have access to data stored in the cloud, the key can be distributed to cloud users through the use of correct key management procedures.

DOI : https://doi.org/10.56452/7-12-34

REFERENCES: -

1. Kaur Amanpreet, Singh, V. P. and Sukhpal Singh Gill. "The future of cloud computing: opportunities, challenges and research trends.", 2018, 2 nd International Conference on, pp. 213-219. IEEE.
2. Rittinghouse, J.W. and Ransome, J.F., Cloud computing: implementation, management, and security. CRC Press, 2017.
3. Hussein, N.H. and Khalid, A., A survey of cloud computing security challenges and solutions. International Journal of Computer Science and Information Security, 2016, 14(1), p.52.
4. Ahmed, Monjur, and Mohammad Ashraf Hossain. "Cloud computing and security issues in the cloud." International Journal of Network Security & Its Applications 6.1 (2014): 25.
5. Jain S, Kumar R, Kumawat S and Jangir S K, “An analysis of security and privacy issues, Challenges with possible solution in cloud computing”, Proc. of the National Conf. on Computational and Mathematical Sciences (COMPUTATIAIV), 2014, 1-7.
6. Sadiku Matthew, N. O., Sarhan M. Musa and Omonowo D. Momoh. "Cloud Computing: Opportunities and Challenges", IEEE Potentials 33, No. 1, 2014, 34-36.
7. Azodolmolky Siamak, Philipp Wieder, and Ramin Yahyapour. "Cloud computing networking: Challenges and opportunitiesfor innovations." IEEE Communications Magazine 51, No. 7, 2013, 54-62.
8. A. Bouayad, A. Blilat, N. E. H. Mejhed and M. El Ghazi, "Cloud computing: Security challenges," 2012 Colloquium in Information Science and Technology, Fez, 2012, pp. 26-31.
9. Eystein Mathisen. Security Challenges and Solutions in Cloud Computing, in: International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011), 2011.p.208-212.
10. Choubey R, Dubey R and Bhattacharjee J, “A survey on cloud computing security challenges and threats” published in International Journal on Computer Science and Engineering (IJCSE), vol.3, 2011, 1227-1231.
11. Farhan Bashir Shaikh and S. Haider, "Security threats in cloud computing," 2011 International Conference for Internet Technology and Secured Transactions, Abu Dhabi, 2011, pp. 214-219.
12. Kuo, Mu-Hsing. "Opportunities and challenges of cloud computing to improve health care services." Journal of Medical Internet Research, 13, No. 3, 2011, e67.
13. K. Popović and Ž. Hocenski, "Cloud computing security issues and challenges," The 33rd International Convention MIPRO, Opatija, 2010, pp. 344-349
14. Wei, Yi, and M. Brian Blake. "Service-oriented computing and cloud computing: Challenges and opportunities." IEEE Internet Computing, 14, No. 6, 2010, 72-75.
15. Choo, K.-K. R. (2010) ‘Cloud computing: Challenges and future directions’, Trends and Issues in Crime and Criminal justice, (400), pp. 1–6.