ISSN 2313-1527 (PRINT)
ISSN 2313-1535 (ONLINE)

IJEIE

International Journal of Electronics
and Information Engineering

Vol. 1, No. 2 (Dec. 2014)

INTERNATIONAL JOURNAL OF ELECTRONICS & INFORMATION ENGINEERING

PUBLISHING OFFICE

Min-Shiang Hwang
Department of Computer Science & Information Engineering, Asia University, Taichung 41354, Taiwan, R.O.C.
Email: mshwang@asia.edu.tw

International Journal of Electronics and Information Engineering is published both in traditional paper form (ISSN 2313-1527) and in Internet (ISSN 2313-1535) at http://ijeie.jalaxy.com.tw

PUBLISHER: Candy C. H. Lin

23-75, P.O. Box, Taichung, Taiwan 40199, R.O.C.

International Journal of Electronics and Information Engineering

Vol. 1, No. 2 (Dec. 2014)

Mobile Cloud Computing Framework for Elastic Partitioned/Modularized Applications Mobility

Salah M El-Sayed[1], Hatem M. Abdul Kader[2], Mohie M. Hadhoud[3], Diaa Salama AbdElminaam[4]
(Corresponding author: Hatem M. Abdul Kader)

Scientific Computing Department, Computers and Informatics, Banha University, Egypt[1]
(ms4elsayed@fci.bu.edu.eg)
Information Systems Department, Faculty of Computers and Informatics, Menofyia University, Egypt[2]
Information Technology Department, Faculty of Computers and Informatics, Menofyia University, Egypt[3]
Information Systems Department, Faculty of Computers and Informatics, Banha University, Egypt[4]

(Received Jan. 27, 2014; revised and accepted May 4, 2014)

Abstract

Mobile applications are becoming increasingly ubiquitous and provide ever richer functionality on mobile devices. At the same time, such devices often enjoy strong connectivity with more powerful machines ranging from laptops and desktops to commercial clouds. Despite increasing usage of mobile computing; using its full potential is difficult due to its inherent problems such as limited resource. Cloud computing can address these problems by executing mobile applications on resource providers external to the mobile device. The foundation of cloud computing is the delivery of services, software and processing capacity over the Internet, reducing cost, increasing storage, automating systems, decoupling of service delivery from underlying technology, and providing flexibility and mobility of information

In this paper, we developed an architecture that uses cloud to do computations that consume resources badly on mobiles. It aims at finding the right spots in an application automatically where the execution can be partitioned and migrated to the cloud. Thus, an elastic application can augment the capabilities of a mobile device including computation power, storage, and network bandwidth, with the light of dynamic execution configuration according to device's status memory, and battery level. We demonstrate results of the proposed application model using data collected from one of our elastic application.

Keywords —Cloud computing, GPS, mobile cloud computing (MCC), offloading, partitioning and migration

1 Introduction

Mobile cloud computing is the cloud structure where the computation and hardware are moved departed from mobile devices .Mobile devices and applications acquire enjoyed rapid development in past years but mobile devices comfort cannot run data qualifier applications, much as search, large-scale information management and defense, etc., and have limitations in battery cognition, screen situation, wireless communication etc.

In primary, the energy render from the controlled battery ability [1] has been one of the most stimulating arrangement issues with mobile device. Thence, program decisions for mobile applications have to accept considerateness of the resource regulating in the pattern.

The emerging cloud computing field [2] offers a tense the capabilities of mobile device for energy-hungry salient applications. Different cloud-assisted mobile platforms acquire been planned, specified as cloudlet [3], cloud copy [4], and etc. In primary, each design is related with a system-level clone in a structure.

The mobile clone, which runs on a virtual Machine (VM), can effect mobile applications on behalf of the mobile device. This structure requires both a performance to apply task offloading and a contract to adjudicate when to offload applications. Existing investigate [5, 6, 7, 8] has proposed a show of application-offloading mechanisms. Nonetheless, the search on best policies for remedy offloading to cloud process is constricted in that they mostly take an unchangeable computing planning in the device and a fixed bandwidth model for the wireless canalize [9]. Mobile cloud technology (Figure.1) brings new types of services and facilities for mobile users to take full advantages of cloud computing. This paper introduces the basic terminology of cloud computing and mobile cloud computing, its background, key technology, current research status, and its further research perspectives as well. We focused on the problem of energy-optimal application execution in the cloud-assisted mobile platform. The objective is to minimize the total resources consumed by the mobile device such as memory, time, and power consumed.

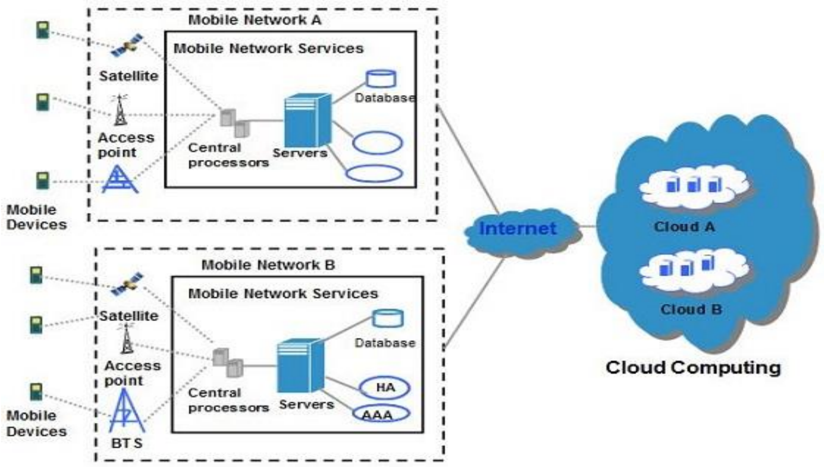


Figure 1: Mobile cloud computing (MCC)

The rest of the paper is organized as follows. Section 2 present cloud computing definitions and basic terminology of mobile cloud computing and its architectures Following that, respectively in the next section the discussion of related work of mobile cloud computing. Following that, respectively in the in Section 4 present problem definitions and system model, and the description of partition cost module and the evaluation. Finally, the conclusion lies in the last section.

2 Background

In order to help us better understanding of Mobile Cloud Computing, let's start from the two previous techniques: Mobile Computing and Cloud Computing followed by mobile cloud computing.

A. *Mobile Computing*
B. *Cloud Computing*
C. *Mobile Cloud computing*

A. *Mobile Computing*

Mobility has become a very popular word and rapidly increasing part in today's computing area. An incredible growth has appeared in the development of mobile devices such as, smartphone, PDA, GPS Navigation and laptops with a variety of mobile computing, networking and security technologies. In addition, with the development of wireless technology like WiMax, Ad Hoc Network and WIFI, users may be surfing the Internet much easier but not limited by the cables as before. Thus, those mobile devices have been accepted by more and more people as their first choice of working and entertainment in their daily lives. So, Mobile computing can described as a form of human-computer interaction by which a computer is expected to be transported during normal usage [10]. Mobile computing is based on a collection of three major concepts: hardware, software and communication. The concepts of hardware can be considered as mobile devices, such as smartphone and laptop, or their mobile components. Software of mobile computing is the numerous mobile applications in the devices, such as the mobile browser, anti-virus software and games. The communication issue includes the infrastructure of mobile networks, protocols and data delivery in their use. They must be transparent to end users. Mobile computing has the following Feature:

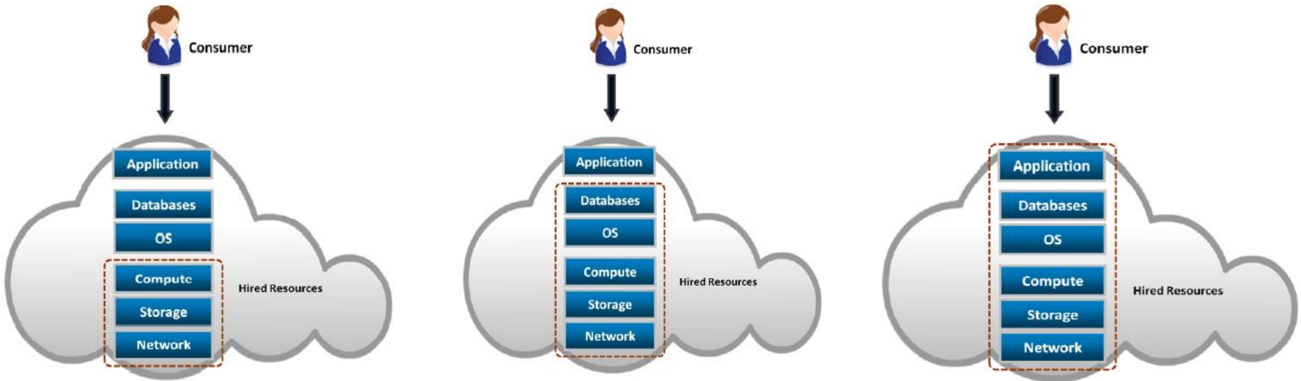
- Mobility
- Diversity of network conditions
- Frequent disconnection and consistency
- Dis-symmetrical network communication
- Low reliability

B. *Cloud Computing*

Cloud Computing is a general term used to describe a new class of network based computing that takes place over the Internet, basically a step on from Utility Computing. In other words, this is a collection/group of integrated and networked hardware, software and Internet infrastructure (called a platform).Using the Internet for communication and transport provides hardware, software and networking services to clients (Figure 2).These platforms hide the complexity and details of the underlying infrastructure from users and applications by providing very simple graphical interface or API (Applications Programming Interface). In addition, the platform provides on demand services that are always on, anywhere, anytime and anyplace. Pay for use and as needed, elastic (scale up and down in capacity and functionalities). The hardware and software services are available to the general public, enterprises, corporations and businesses markets. The term Private Cloud is used when the cloud infrastructure is operated solely for a business or an organization. A composition of the two types (private and public) is called a Hybrid Cloud, where a private cloud is able to maintain high service availability by scaling up their system with externally provisioned resources from a public cloud when there are rapid workload fluctuations or hardware failures.

In general, cloud providers fall into three categories as shown in Figures 2(a), 2(b), and 2(c) (that show the comparison of different type of services provided by cloud computing):

- *Infrastructure as a Service (IaaS)*: offering web-based access to storage and computing power. The consumer does not need to manage or control the underlying cloud infrastructure but has control over the operating systems, storage, and deployed applications.
- *Platform as a Service (PaaS):* giving developers the tools to build and host web applications (e.g., APPRIO [11], software as a service provider, is built using the Force.com [12] platform while the infrastructure is provided by the Amazon Web Service [13]). The users host an environment for their applications. The users control the applications, but do not control the operating system, hardware or network infrastructure, which they are using.
- *Software as a Service (SaaS):* where the consumer uses an application, but does not control the operating system, hardware or network infrastructure. In this situation, the user steers applications over the network. Applications that are accessible from various client devices through a thin client interface such as a web browser.



(a) Infrastructure as a Service (IaaS): (b) Platform as a Service (PaaS): (c) Software as a Service (SaaS)

Figure 2: The cloud computing services models

C. *Mobile Cloud computing*

There are several definitions of mobile cloud computing [14, 15], and different research refers to different concepts of the mobile cloud.The term mobile cloud computing means:

The combination of cloud computing and mobile networks to bring benefits for mobile users, network operators, as well as cloud providers. Cloud computing exists when tasks and data are kept on the Internet rather than on individual devices, providing on-demand access. Mobile cloud computing can involve other mobile devices and/or servers accessed via the Internet. A related notion is cloudlets, which has been viewed in different ways [16, 17]. Applications are run on a remote server and then sent to the user. Because of the advanced improvement in mobile browsers thanks to Apple, Google, Microsoft and Research in Motion, nearly every mobile should have a suitable browser. This means developers will have a much wider market and they can bypass the restrictions created by mobile operating systems. Mobile cloud computing gives new company chances for mobile network providers. Several operators such as Vodafone, Orange and Verizon have started to offer cloud computing services for companies [18].

3 Related Works

To give more prospective about the Mobile Cloud Computing, this section discusses the results obtained from other resources.

It was shown in [19] executes video games in the cloud and delivers video stream to resource-poor clients without interrupting the game experience. Many other examples where the cloud can augment mobile devices can be envisioned, e.g. virus scan, mobile file system indexing, augmented reality applications.

In [20] uses VM migration to offload part of their application workload to a resourceful server through either 3G or WiFi. CloneCloud was tested using Android phones with the clones executing on a Dell desktop running Ubuntu. The system is a flexible application partitioned and execution runtime. It enables unmodified mobile applications to offload part of their execution from mobile devices onto device clones operating in a computational cloud.

It was presented in [21] ‘Hyrax’ for Android smartphone applications which are distributed both in terms of data and computation based on Hadoop ported to the Android platform. Hyrax explores the possibility of using a cluster of mobile phones as resource providers and shows the feasibility of such a mobile cloud. As a sample application, they present 'HyraxTube'; which is a simple distributed mobile multimedia search and sharing program. The objective of HyraxTube is to allow users to search through multimedia files in terms of time, quality, and location.

AlfredO [22] is a middleware platform to automatically distribute different layers of application in smartphones and cloud, respectively, by modeling applications as a consumption graph, and finding the optimal modules. The test result shows that such platform improves the performance of applications in cloud computing effectively. AlfredO system consists of three bundles (the interface encapsulation on Java classes and services): AlfredOClient and Renderer on the client and AlfredO Core on the server (shown in Figure 3). There are several of researches about Mobile Cloud Computing can be found in [23, 24, 25]

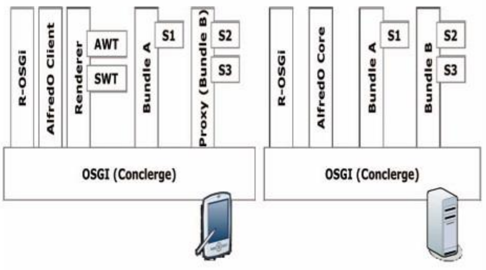


Figure 3: AlfredO architecture

4 Problem Definition and System Model

In this section, we present a model for application execution on the cloud-assisted mobile application platform. Application system architecture as shown in Fig.5, First, we define a mobile application profile. Then, we calculate consuming resources for application execution, including resources consumed for computation on mobile execution and a transmission computation to cloud execution. The following Sequence steps for our framework application as shown in (Figure 4) .We use a mobile smartphone SAMSUNG GALAXY GRAND 1.2 GHz Dual Core CPU, and Android 4 Operating Systems in which performance data is collected and tested. In the experiments, the PartotionMigrate2Cloud application smartphone calculate some of GPS calculations such as distance between two points or more till 100 points using different algorithms. For our experiment, we calculate the effects of Sending computation to cloud web service and back with results and studying the Offloading computation to save energy on power consumption for smartphone mobile in case of running all processes of application on mobile or by partition and offloading processes to cloud.

In first step: Comparison is conducted using two different types of GPS mode (using mobile GPS), and using mobile network .for each type of GPS, we can get latitude and longitude for each point (it can be calculated by mobile GPS satellite or by mobile network).in this research we implement the two mode of operations

In second step: After selecting GPS mode of operations, we have to choose between manual or automatic calculation to get latitude or longitude for each point

- If automatic calculation is selected, we have to enter number of points and system get points every thirty second;
- If manual calculation is selected, we have to click to get points.

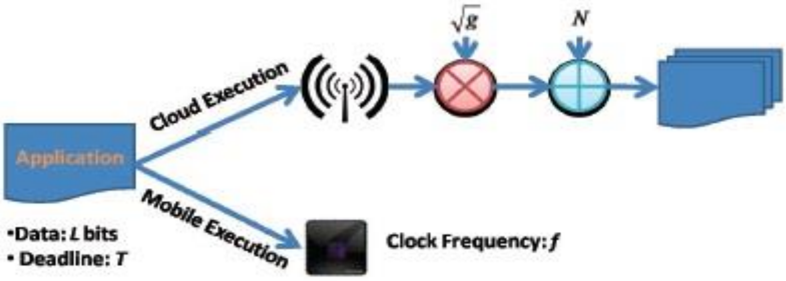


Figure 4: Mobile application excuted in two alternative modes mobile excution (lower) and the cloud excution (upper)

In third step: After selecting method to get points either manually or automatic, we have to choose between calculation way on mobile or by partition and offloading to perform part of calculation on mobile and part on cloud server.

A. In case calculation on mobile, calculation is conducted in case of getting points manually or automatic Mobile Application will take GPS reading and perform calculations over certain period of time:

1). GPS reading to determine latitude and longitude for each point either by GPS for mobile (smart phone) or from mobile network.
2). Then calculate the distance between two point or more using different algorithms.
3). The Application will perform all calculations on smart phone device and calculate the results and the consuming resources such as Memory consumed, CPU usage, Time consumed for calculation, battery consumed to perform the processes, time consumed for calculations and for getting points.

B. In case of partition and Migrations activities or methods to cloud, in this steps application is partition and migrate activities to cloud to consider this application as platform as a services (PaaS) and mobile considered as thin client that enables the mobile applications developers to take decision of performing all application processes on an android mobile device or to divide the application processes to execute on mobile & cloud.
1). GPS reading to determine latitude and longitude for each point either by GPS for mobile (smart phone, satellite) or from mobile network (this step execute on mobile device).
2). Then data (longitude and latitude for each point) is migrated to cloud server to perform calculation on cloud.
3). The distance between two point or more using different algorithms calculations performed on cloud the distance between two point or more using different algorithms.
4). The Application will perform distance calculations on cloud server and calculate the results and the consuming resources such as Memory consumed for sending and receiving results, Memory consumed for distance calculations only, Memory consumed for all process from getting points till receive results, CPU usage, Time consumed for calculation, battery consumed to perform the transmitting data, time consumed for calculations and for getting points.

5 Mathematical Calculation

5.1 Distance Using Haversine Formula

For our experiment, distance calculations between two point using the ‘haversine’ formula to calculate the great-circle distance between two points – that is, the shortest distance over the earth’s surface .The formula assumes that the earth is a sphere, (we know that it is "ellipse " shaped) – giving an ‘as-the-crow-flies’ distance between the points (ignoring any hills, of course!).

- haversine Formula

$$a = \sin^2(\Delta\varphi/2) + \cos(\varphi 1).\cos(\varphi 2).\sin^2(\Delta\lambda/2)$$
$$c = 2.\text{atan2}(\sqrt{a}, \sqrt{(1-a)})$$
$$d = R.c$$

$\Delta\varphi$ is latitude difference (lat2− lat1), $\Delta\lambda$ is longitude difference (long2− long1), R is earth’s radius(mean radius = 6,371km).

5.2 Distance Using Spherical Low of Cosines

When Sinnott published the haversine formula, computational precision was limited. Nowadays, most modern computers & languages use IEEE 754 64-bit floating-point numbers, which provide 15 significant figures of precision. With this precision, the simple spherical law of cosines formula gives well-conditioned results down to distances as small as around 1 metre:

- spherical law of cosines formula

$$\mathbf{d = acos(sin(\varphi_1).sin(\varphi_2) + cos(\varphi_1).cos(\varphi_2).cos(\Delta\lambda)).R}$$

5.3 Distance Using Equirectangular Approximation

If performance is an issue and accuracy less important, for small distances Pythagoras’ theorem can be used on anequirectangular projection:

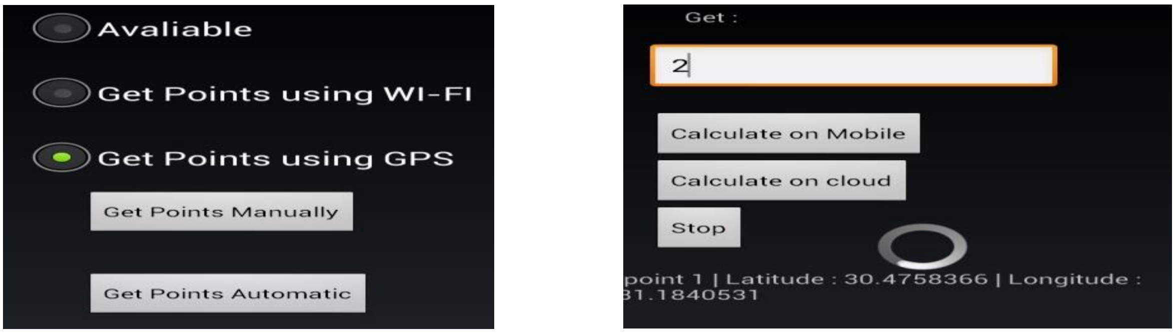
- Formula

$$\mathbf{x = \Delta\lambda.cos(\varphi)}$$
$$\mathbf{y = \Delta\varphi}$$
$$\mathbf{d}= R.\sqrt{(x^2 + y^2)}$$

6 Experiment (Automatic Calculations)

6.1 Getting Points Using GPS Satellite

Figures 5(a) and 5(b) show the main interface for all steps of the application in case of getting points automatic using GPS satellite.


○ Avaliable

○ Get Points using WI-FI

● Get Points using GPS

Get : 2

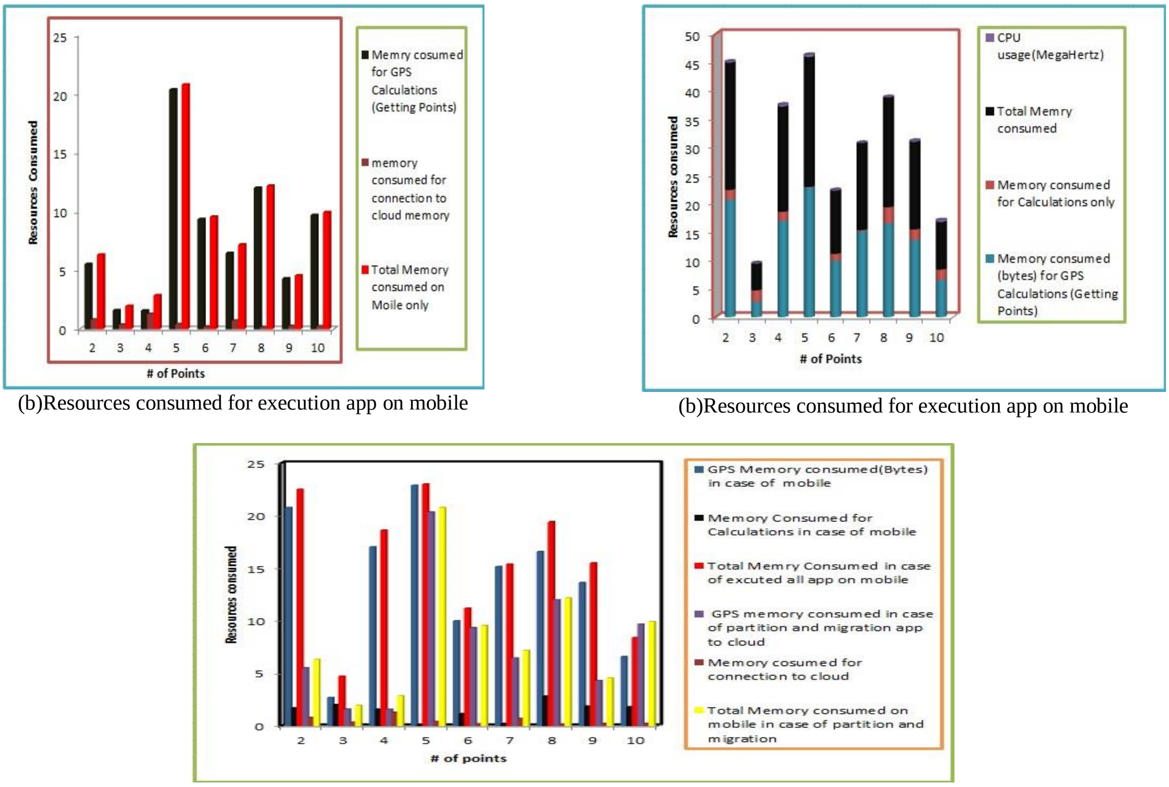
point 1 | Latitude : 30.4758366 | Longitude : 31.1840531

(a) Getting points (latitude and Longitude) using mobile GPS satellite

(b)Getting points automatic(every 30 Sec)

Figure 5: Snapshot of elastic GPS application on Samsung Galaxy grand

Table 1 shows resources consumed in case of automatic calculation in case of getting longitude and latitude for each point automatically every 30 second using GPS satellite for execution application on cloud web services and the for different number of points range from two points till ten points (GPS calculation on mobile smartphone and calculation migrated to cloud and return results to mobile).



(b)Resources consumed for execution app on mobile

(b)Resources consumed for execution app on mobile

(c) Memory consumed for execution application on mobile and cloud

Figure 6: Resources consumed for automatic calculation for Getting Points using GPS satellite

Figures 6(a), 6(b), and 6(c) show the experimental results for different data calculations using automatic method for getting longitude and latitude for each point rang from calculating distance between two points till ten points in case of distancing range from approximately 50 meter till 200 meter in case of all calculation done on mobile device or application is partitioned and offloading on cloud to perform distance calculation on cloud.

Table 1 and Figure 6(a) show the results of execute all application processes on mobile smartphone only. The results include the following matrices:

- Memory consumed for GPS calculation only (getting longitude and latitude for each point).
- Memory consumed for calculating distances between points.
- Total Memory consumed to execute app.
- Time consumed and CPU usage for calculations.

Figure 6(b) shows the results of partitioned and migrate activities to web services. The results include the following matrices:

- Memory consumed on mobile for getting longitude and latitude for each point.
- Memory consumed on cloud (bytes) for calculating distances between points on cloud.
- Memory consumed for send points longitudes and latitudes to web services or receive results from web services to mobile smart phone.
- Total memory consumed on mobile smartphone for calculations.

Table 1: Resources consumed for execution application on mobile smartphone and cloud web services (getting points using GPS satellite)

Automatic calculation for Getting Points using GPS Satellite																		
	Mobile Calculations								Cloud Calculations									
	Memory Consumed(bytes)			Time(sec)		Battery(percent)		CPU		Memory Consumed(bytes)				Time(sec)		Battery(percent)		
# points	GPS Calculations (Getting Points)	Calculations	Total Memory	GPS Calculations (Getting Points)	Calculations	Battery used for Calculations	Total Battery consumed	CPU usage(Megahertz)	# of points	GPS Calculations (Getting Points)	connection to cloud memory	Memory consumed for calculation only	Total Memory on Mobile	GPS Calculations (Getting Points)	Connection to Cloud	GPS Calculations (Getting Points)	Connection to Cloud	Total Battery
2	20.769531	1.71875	22.488281	30	1	0.0%	0.0%	0.18474126	2	5.5117188	0.8046875	104.21875	6.3164063	30	2	0.0%	0.0%	0.0%
3	2.703125	2.03125	4.734375	60	1	0.0%	0.0%	0.08333331	3	1.5898438	0.3671875	103.22875	1.9570313	60	1	0.0%	0.0%	0.0%
4	17.019531	1.5898438	18.6093748	90	1	0.0%	1.0%	0.33726683	4	1.5742188	1.2851563	105.0625	2.8593751	90	5	1.0%	0.0%	1.0%
5	22.875	0.11328125	22.98828125	120	1	0.0%	0.0%	0.3783784	5	20.332031	0.421875	105.0859375	20.753906	120	1	0.0%	0.0%	0.0%
6	10	1.1825	11.1825	150	1	0.0%	0.0%	0.09859155	6	9.3359375	0.203125	105.9140625	9.5390625	150	1	0.0%	0.0%	0.0%
7	15.15625	0.23046875	15.38671875	180	1	0.0%	1.0%	0.034909904	7	6.4580313	0.70703125	105.9140625	7.16506255	180	1	1.0%	0.0%	1.0%
8	16.5703125	2.8425	19.4128125	210	1	0.0%	1.0%	0.07042256	8	11.9921875	0.171875	106.765625	12.1640625	180	1	1.0%	0.0%	1.0%
9	13.6210938	1.87595	15.4970438	240	1	0.0%	2.0%	0.1722334	9	4.3007813	0.24609375	106.765625	4.54687505	240	2	2.0%	0.0%	2.0%
10	6.5976563	1.8164063	8.4140626	300	1	0.0%	1.0%	0.30555555	10	9.675781	0.23828125	107.6171875	9.91406225	300	1	1.0%	0.0%	1.0%

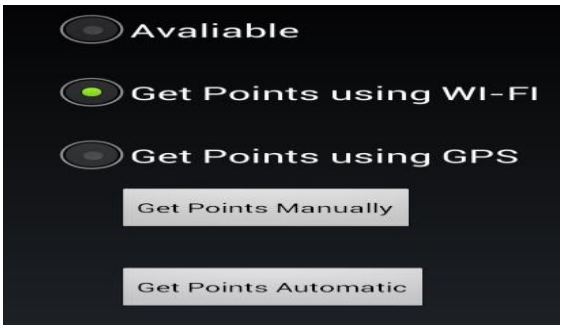
The performance of execute application on mobile or cloud in terms of memory consumed using different distance and number of points are shown in Fig 6(c).the total memory consumed on mobile in the case of cloud or in the case of executed all the application on mobile only. According to partition and migrate app to cloud, most of resources consumed on mobile smartphone will decrease approximately to the half as shown in Figure 6(c). In case of partition and offloading application most of resources consumed on cloud and minimize the resources consumed in mobile smartphone.

6.2 Getting Points Using Network GPS

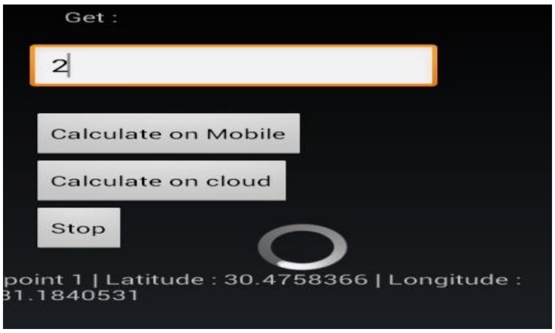
Figures 7(a) and 5(b) show the main interface for all steps of the application in case of getting points automatic using network GPS. Table 2 shows resources consumed in case of automatic calculation in case of getting longitude and latitude for each point automatically every 30 second using network GPS for execution application on cloud web services and the for different number of points range from two points till ten points.

Table 2: Resources consumed for execution application on mobile smartphone and cloud web services (Getting points using GPS satellite)

	Automatic calculation for Getting Points using Network GPS																	
	Mobile Calculations								Cloud Calculations									
	Memory Consumed(bytes)			Time(sec)		Battery(percent)		CPU		Memory Consumed(bytes)				Time(sec)		Battery(percent)		
# points	GPS Calculations (Getting Points)	Calculations	Total Memory	GPS Calculations (Getting Points)	Calculations	Battery used for Calculations	Total Battery consumed	CPU usage(Megahertz)	# of points	GPS Calculations (Getting Points)	connection to cloud memory	Memory consumed for calculation only	Total Memory on Mobile	GPS Calculations (Getting Points)	Connection to Cloud	GPS Calculations (Getting Points)	Connection to Cloud	Total Battery
2	11.7503125	1.1914063	12.9417188	30	1	0.0%	1.0%	0.22927971	2	1.7539063	0.5742187	103.8984375	2.328125	30	3	1.0%	0.0%	1.0%
3	13.464844	0.53125	13.996094	60	1	0.0%	0.0%	0.04198918	3	4.78215	0.08203215	103.8984375	4.86418215	60	3	0.0%	0.0%	0.0%
4	10.5078125	8.167969	18.6757815	90	1	1.0%	1.0%	0.029733963	4	6.234375	0.1328215	104.8515625	6.3671965	90	1	1.0%	0.0%	1.0%
5	5.7890625	0.12109375	5.91015625	120	1	0.0%	0.0%	0.0833334	5	4.421875	0.07206275	104.8515625	4.49393775	120	1	0.0%	0.0%	0.0%
6	4.2109375	0.29296875	4.50390625	150	1	0.0%	1.0%	0.10329509	6	3.316406	0.0585937	105.828125	3.3749997	150	1	1.0%	0.0%	1.0%
7	4.27343375	0.15625	4.42968375	180	1	0.0%	1.0%	0.28092882	7	1.890625	0.33203125	105.727315	2.22265625	180	1	1.0%	0.0%	1.0%
8	6.6757813	0.03125	6.7070313	210	1	0.0%	1.0%	0.097793005	8	5.980469	0.0546875	106.796875	6.0351565	180	1	1.0%	0.0%	1.0%
9	12.5117188	10.40625	22.9179688	240	1	0.0%	1.0%	0.05405406	9	11.453125	1.234375	107.2578125	12.6875	240	3	1.0%	0.0%	1.0%
10	4.0429688	0.390625	4.4335938	270	1	0.0%	2.0%	0.49080235	10	3.5703125	0.3046875	108.25	3.875	270	1	2.0%	0.0%	2.0%



(a) Getting points (latitude and longitude) using mobile network GPS

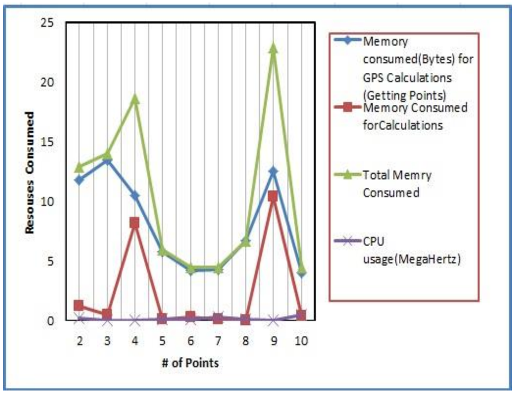


point 1 | Latitude : 30.4758366 | Longitude : 31.1840531

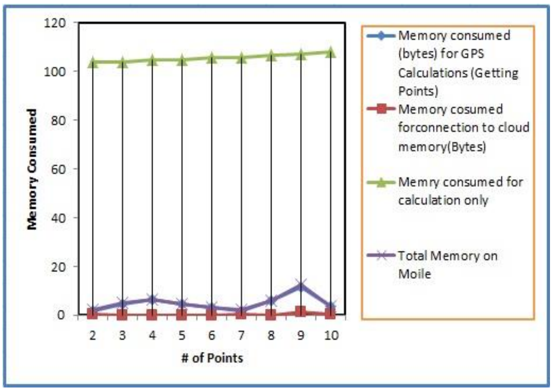
(b)Getting points automatic(every 30 Sec)

Figure 7: Snapshot of elastic GPS application on Samsung Galaxy grand

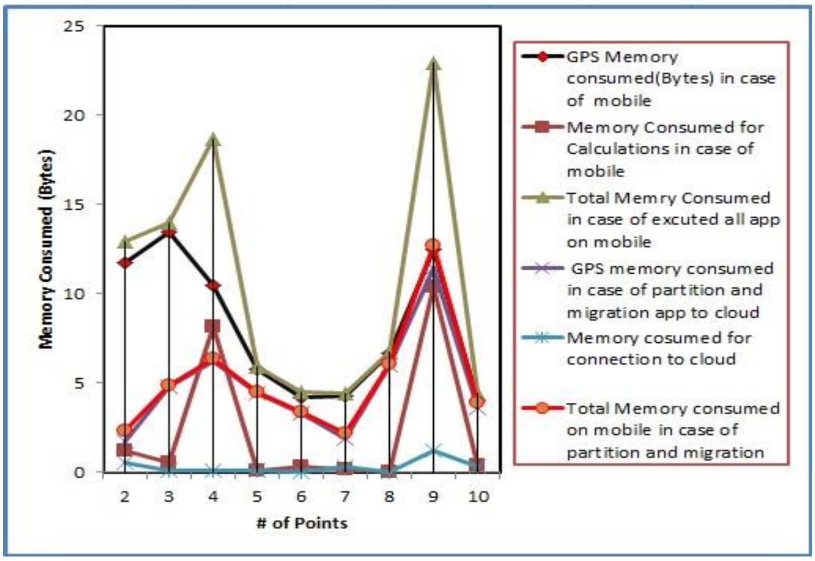
Figures 8 shows the experimental results for different data calculations using automatic method for getting longitude and latitude for each point rang from calculating distance between two points till ten points in case of distance range from approximately 50 meter till 200 meter in case of all calculation done on mobile device or application is partitioned and offloading on cloud to perform distance calculation on cloud.



(b)Resources consumed for execution app on mobile



(b)Resources consumed for execution app on mobile



(c) Memory consumed for execution application on mobile and cloud

Figure 8: Resources consumed for automatic calculation for getting points using network GPS

– Figure 8(a) shows the results of execute all application processes on mobile smartphone only. The results include as the same as in case of getting point using GPS Satellite such as memory consumed for getting points only, memory consumed for calculations only, CPU usage for calculation, and Time consumed.
– Figure 8(b) shows the results of partitioned and offloading application on cloud. The results include as the same as in case of getting point using GPS Satellite.
– Figure b(c) shows The performance of execute application on mobile or cloud in terms of memory consumed using different distance and number of points .According to partition algorithm, most of resources consumed on mobile smartphone will decrease approximately to the half. In case of partition and offloading application most of resources consumed on cloud and minimize the resources consumed in mobile smartphone.

7 Conclusion and Future Work

In this paper, we proposed the elastic partition algorithm and partition cost module. Partition and migrate activities and method from mobile smartphone to cloud web services is a good idea and may reduce resources on mobile. Thus, cloud computing can save energy for mobile users through computation offloading. Cloud computing can used for extending battery lifetime (Computation offloading migrates large computations and complex processing from resource-limited devices (i.e., mobile devices) to resourceful machines (i.e., servers in clouds)). Remote application execution can save energy significantly. Also CC can help in improving data storage capacity and processing power. MCC enables mobile users to store/access large data on cloud. It can help in reduce the running cost for computation intensive applications. Those results by mobile applications are not constrained by storage capacity on the devices because their data now is stored on the cloud.

In future we will consider smartphone devices as thin clients and migrate all app automatically to cloud web services that can help in improving reliability and availability (Keeping data and application in the clouds reduces the chance of lost on the mobile devices). CC can also increase scalability (Mobile applications can be performed and scaled to meet the unpredictable user demands, Service providers can easily add and expand a service).

Acknowledgments

This study was supported by the Faculty of computer and informatics (Benha University, Menofyia University). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1]. A. P. Miettinen and J. K. Nurminen, ”Energy efficiency of mobile clients in cloud computing,” *in Proceedings of the 2nd USENIX conference on hot topics in cloud computing*, Berkeley, CA, USA, 2010.

[2]. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, ”A view of cloud computing”, *Communication of the ACM, vol.* 53, no. 4, pp.50-58, 2010.

[3]. M. Satyanarayanan , P. Bahl, R. Caceres , and N. Davies,”The case for VM-based cloudlets in mobile computing,” *IEEE Pervasive Computing*, vol. 8, no. 4, pp. 14-23, Oct.-Dec. 2009.

[4]. B. G. Chun, and P. Maniatis,”Augmented smartphone applications through clone cloud execution,” *in Proceedings of the 12th Conference on Hot Topics in Operating Systems*, Berkeley, CA, USA, 2009.

[5]. R. K. Balan,”The case for cyber foraging,” in *Proceedings of 10th ACM Special Interest Group on Operating Systems European Workshop (SIGOPS)*, ACM Process, pp. 87-92, 2002.

[6]. M. Satyanarayanan, ”Pervasive computing: Vision and challenges,” *IEEE Personal Communication*, vol. 8, no. 4, pp. 10-17, 2001.

[7]. B. G. Chun, S. H. Ihm, P. Maniatis, M. Naik, and A. Patti, ”CloneCloud: Elastic execution between mobile device and cloud,” *in Proceedings of the 6th European Conference on Computer Systems* (EuroSys 2011), Apr. 2011.

[8]. X. W. Zhang, A. Kunjithapatham, S. Jeong and S. Gibbs, ”Towards an elastic application model for augmenting the computing capabilities of mobile devices with cloud computing,” *Mobile Network Applications*, vol. 16, pp. 270-284, 2011.

[9]. K. Kumar, and Y. H. Lu,”Cloud computing for mobile users: can offloading computation save energy?” *IEEE Computer*, vol. 43, no.4, pp. 51-56, Apr. 2010.

[10]. M. Satyanarayanan, ”Fundamental challenges in mobile computing”, in Proceedings of the Fifteenth Annual ACM Symposium on Principles of Distributed Computing (PODC’96), ACM, New York, NY, USA, pp. 1–7, 1996.

[11]. APPRIO Homepage : last accessed 13, Oct. 2013. (http://www.appirio.com/)

[12]. Force.com Homepage : last accessed 13, Oct. 2013. (http://www.salesforce.com/platform/)

[13]. Amazon Web Services : last accessed 13, Oct. 2013. (http://aws.amazon.com/)

[14]. E. P. Daniela, M. L. Alina, “Mobile cloud computing”, Book Chapter in “New Trends in Mobile and Web Development 2012”, Publication series of Lahti University of Applied Sciences, ISBN 978-951-827-141-6, Chapter 10, pp. 287-336, 2012.

[15]. F. Xiaopeng, C. Jiannong, and M. Haixia, "A survey of mobile cloud computing", *ZTE Communications, Special Issue on Mobile Cloud Computing and Applications*, vol. 9, no. 1, pp. 4-8, 2011.

[16]. L. Guan, K. Xu, S. Meina, and S. Junde, “A survey of research on mobile cloud computing”, in *IEEE/ACIS 10th International Conference on Computer and Information Science (ICIS),* pp. 387-392, 2010.

[17]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, ”Above the clouds: A berkeley view of cloud computing”, *Technical Report UCB/EECS-2009-28, University of California, Berkeley*, Feb. 2009.

[18]. F. Niroshinie, W. L. Seng, R. Wenny, ”Mobile cloud computing: A survey”, *Future Generation Computer Systems*, vol. 29, no. 1, pp. 84-106, Jan. 2013.

[19]. OnLive Inc., “OnLIve.” [Online]. Available: http://www.onlive.com

[20]. G. C. Byung, I. Sunghwan, M. Petros, “Clonecloud: Elastic execution between mobile device and cloud”, in *Proceedings of the Sixth Conference on Computer Systems (EuroSys’11)*, ACM, New York, NY, USA, pp. 301–314, 2011.

[21]. E. E. Marinelli, ”Hyrax: Cloud computing on mobile devices using MapReduce”, *Masters Thesis*, Carnegie Mellon University, 2009.

[22]. I. Giurgiu, O. Riva, D. Juric, I. Krivulev, G. Alonso, ”Calling the cloud: enabling mobile phones as interfaces to cloud applications”, in *Bacon, J. M., Cooper, B. F. (eds.), LNCS, Springer, Heidelberg*, vol. 5896, pp. 83–102, 2009.

[23]. G. H. Canepa, D. Lee, ”A virtual cloud computing provider for mobile devices”, in *Proc. of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond*, 2010.

[24]. M. Satyanarayanan, P. Bahl, R. Caceres, N. Davies, ”The case for vm-based cloudlets in mobile computing”, *Proc. IEEE Pervasive Computing*, vol. 8, no. 4, pp. 14–23, 2009.

[25]. D. Kovachev, Y. Tian, R. Klamma, ”Adaptive computation offloading from mobile devices into the cloud,” in *IEEE 10th International Symposium on Parallel and Distributed Processing with Applications (ISPA)*, pp. 784-791, 10-13 July 2012.

Salah M. Elsayed, Dean, Faculty of Computers and Information, head of Scientific Computing Department, Benha University, Benha, Egypt. His PhD degree, in Numerical Analysis from the department of Numerical, Theory and Algorithms of Numerical Linear Algebra, and numerical methods of ordinary and partial differential equations (multi-integral and finite difference methods. A domain decomposition method and chebychev pseudo spec trail methods. Prof Salah obtain Egyptian incentive prize of science in mathematics 2002,and Scopus prize of Best Author have higher citation and H-Index in Scopus 2008 in the last ten years. Prof. Salah has published more than 150 papers in international journals, international conferences, local journals and local conferences. His fields of Interest: Numerical Analysis, numerical methods of ordinary and partial differential equations, and Information security and data hiding.

Hatem. M. Abdul-kader vice Dean of Faculty of Computers and Information, Menoufia university, Shebin Elkom, Egypt. Prof Hatem obtained his BSC. And M.SC. (by research) both in Electrical Engineering from the Alexandria University, Faculty of Engineering, Egypt in 1990 and 1995 respectively. He obtained his Ph.D. degree in Electrical Engineering also from Alexandria University, Faculty of Engineering, in 2001 specializing in neural networks and applications. Since 2009 he is the Head of the department of Information Systems (IS). Prof. Hatem has published more than 100 papers in international journals, international conferences, local journals and local conferences. He is currently a Professor in Information systems department, Faculty of Computers and Information, Menoufya University, Egypt since 2004.

Mohiy Mohamed Hadhoud, Former vice president of Menoufia university for education and student affairs and former dean of Faculty of Computers and Information, University, Shebin Elkom, Egypt. Currently, he is the dean of Canadian International College (CIC) in New Cairo. He is a member of National Promotion committee for professors, he is a member of National Computers and Informatics Sector Planning committee, and is the University training supervisor. Prof Hadhoud graduated from the department of Electronics and Computer Science, Southampton University, UK, 1987. Since 2001 he worked as a Professor of Multimedia, Signals and image processing and Head of the department of Information Technology (IT), He was a member of the university council. He is the recipient of the university supremacy award for the year 2007. He, among others are the recipient of the Most cited paper award from the Digital signal processing journal, Vol.18, No. 4, July 2008, pp 677-678, ELSEVIER Publisher. Prof. Hadhoud has published more than 160 papers in international journals, international conferences, local journals and local conferences. His fields of Interest: Digital Signal Processing, 2-D Adaptive filtering, Digital Image Processing, Digital communications, Multimedia applications, Information security and data hiding.

Diaa Salama Abdul-Minaam was born on November 23, 1982 in KafrSakr, Sharkia, Egypt. He received the B.S from Faculty of Computers &Informatics, Zagazig University, Egypt in 2004 with grade very good with honor, and obtains master degree in information system from faculty of computers and information, menufia university, Egypt in 2009 and submitted for PhD from October 2009. He is working in Benha University, Egypt as teaching assistance at Faculty of Computer and informatics. Diaa has contributed more than 18+ technical papers in the areas of wireless networks, wireless network security, Information security and Internet applications in international journals, international conferences, local journals and local conferences. He majors in Cryptography and Network Security. (Mobile: +20166104747 E-mail: ds_desert@yahoo.com).

Common Techniques and Tools for the Analysis of Open Source Software in Order to Detect Code Clones: A Study

Hamed Jelodar[1], Javad Aramideh[2]
(Corresponding author: Hamed Jelodar)

Department of Computer, Science and Research, Islamic Azad University, Bushehr, Iran[1]
(Email :Jelodarh@gmail.com)
Department of Computer, Islamic Azad University, Sari branch, Iran[2]

(Received May 27, 2014; revised and accepted July 29, 2014)

Abstract

Code clone detection and its elimination are introduced as an influential factor in improving software quality, especially in large software systems. The code that duplicates and is in similar files of source is called code clone. So far, researchers introduced and presented many tools and techniques to analyze and identify clones. But given the importance of this paper, some common techniques and tools used to identify clones should be examined and 4 open-source software systems are analyzed using CloneDr tool. According to the results, many clones were identified and the results show that further improvements are needed for high quality software.

Keywords: Clone detection; Clone detection tool; Code clone

1 Introduction

Several factors influence the reduction or decrease of software quality. One factor that reduces the quality of software is the existence of code clone is a resource file. It is said that code clone is defined differently and clone means the duplicated codes in a source file. Identifying clones renders gives a substantial assistance to improve the quality of software. Generally, code clones are divided into four types, which referred in the next section. Many different techniques have already been proposed to detect code clones and the most common include Text-based, Token-Based, ASSET-Based, PDG-Based. Also, in order to analyze and identify clones several tools have been introduced to implement and the most popular tools are CCFinder, CloneDr. In this paper, some common techniques and tools to identify clones are examined and finally (4) open source software systems are analyzed. In the second part we will continue with a review of earlier works and in the third and fourth parts the clone is introduced and some common techniques and tools are examined to identify and analyze the clones. The fifth section analyzes four software systems using the tool "CloneDr”. Finally, in the sixth Section the conclusions are discussed.

2 Previous Works

Code clones in software systems lead to lower quality of software. Since it is not possible to easily identify the clone, researchers have developed various tools and techniques to detect clones. This section will point out some of the works associated with the topic. Kamiya and colleagues [1].presented a method for the detection of code clones using token-based technique. Burd and colleagues [2] tried to measure and evaluate clone detection tools and found that each have strengths and weaknesses and suggested a combination of tools to perform analysis. Also, some researchers evaluated open source software systems such as Saha and colleagues who evaluated 17 open source software systems with languages C, Java, and C + + [3]. Calefato and colleagues offered a semi-automated method to identify clones in web applications and the results show that the proposed approach effectively and efficiently to detect clones in web applications [4].

3 Clone Code

One of the major problems in software system is code clones and it is more common in large systems. Code clones are duplicated codes which are useless in software source code [5,6].Code clone is classified into many different types and several techniques have been introduced to identify them and several tools were implemented to isolate clones. Code clone detection applications benefits can include: improving software processes, detecting duplicate code, detecting plagiarism and copyright infringement pointed out [7].

Code clones are generally divided into four categories which include 1. Type one. 2. Type two. 3. Type three. 4. Type four and some techniques are introduced to identify any of these types.

Type 1: Pieces of code that are identical except for whitespace, layout and comments are different.

Type 2: Parts are the same except in writing and identifiers, literals, types, whitespace, layout and comments are different.

Type 3: More changes will be copied components, for example, to change, add or delete the comments, in addition to the name change, literals, types, whitespace.

Type 4: Two or more pieces of code that do the same calculation, but with different methods are carried out.

4 Clone Detection Techniques and Tools

In this section we will introduce some of the techniques and tools to identify clones.

4.1 Common Techniques

There are several techniques for Code clone detection that can be very effective in detecting code clones, introducing four common techniques to detect clones [8].

In Figure 1, some of the most popular tools for identifying clones with respect to the existing methods are shown.

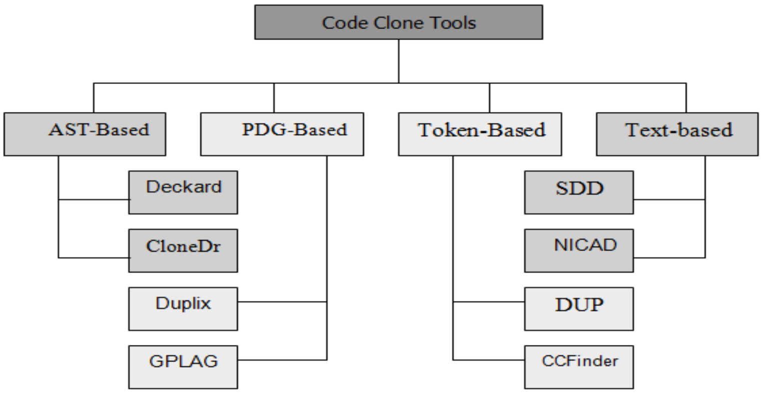


Figure 1: Some popular tools for identifying clones

1) Text-based: In this way, the intended source code is considered as a sequence of lines or strings and two pieces of code to find a sequence of text strings that are similar are compared. When two or more pieces of code had the highest degree of similarity, it will be returned as a clone or clones of a class (as a result). Typically, in this method whitespace and comments are not considered [9].

2) Token-Based: In this method, lexical analysis of source code is discussed, and then the token is to be used as a basis for clone detection [10]. This token can be identifier and literal. This method can detect various types of clones [8, 11].

3) AST-Based: AST-Based compares the same sub-trees. Tree-based methods provide a tree graph of a summary of source code and then search the clone detection algorithm under a tree similar to this "cognitive summary graph" (AST) [12, 13].

4) PDG-Based: This method uses the semantic approach in order to identify clones uses. PDG includes control flow and data flow information of a program [14].

4.2 Available Tools to identify clones

Different tools have been designed for clone detection with different types. While a few of them have been commercialized, many of them are currently used for research purposes to help the software development and maintenance processes. As shown in Figure 1, each of the instruments uses techniques to detect clones. These tools will help us to analyze software systems with multiple languages (such as C #, JAVA) and find the code clones. Some of the most popular of these tools include CCFinder, SimCad, CloneDR, JPlag.

1) Clone detection by CCFinder: CCFinder is one of the tools to detect duplicated codes that are called code clones and are used for the analysis of large-scale systems. With this software, the files source with different languages can be analyzed and these languages include: Java, C / C + +, COBOL, VB, C # [15].

2) Clone detection by CloneDr: CloneDr is a tool that is used to detect code clones. With this tool, you can analyze thousands or millions of lines of code or files. This tool can be used to run the Windows operating system. This tool supports various languages including: Java, C #, C + +, COBOL, JavaScript, PHP [6]. In this paper, using this software we analyze multiple open source software systems, which version of C # is chosen for analysis.

3) Clone detection by Jplag: Jplag is a system that can detect duplicated code in a code source. The tool has a powerful graphical interface to present the results. Currently this tool supports Java, C #, C, C + +, Scheme and natural language text [16].

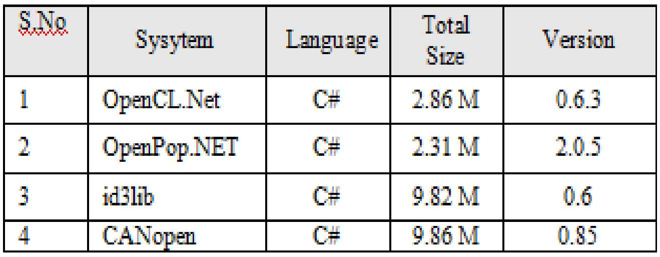
4) Clone detection by SimCad: This tool uses hashing technique to detect code clones and runs through the Eclipse software. SimCad has been used successfully in various fields of research such as Web Mining, text retrieval, etc. [17].

5. Experiments and Results

In this section we evaluated and analyzed multiple open source software systems to detect code clones. To do this, we have analyzed 4 Open Source Software Systems with the3 programming language of C #.

Table 1 shows the information systems that have been selected for analysis And Table 2 is the meanings of the used terms and table 3 is the overall results obtained from the analysis of the software.

Table 1: Systems information

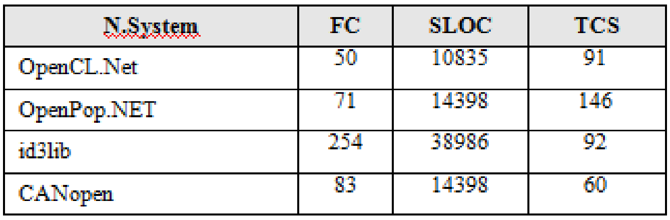


S.No	Sysytem	Language	Total Size	Version
1	OpenCL.Net	C#	2.86 M	0.6.3
2	OpenPop.NET	C#	2.31 M	2.0.5
3	id3lib	C#	9.82 M	0.6
4	CANopen	C#	9.86 M	0.85

Table 2: Meanings of used terms

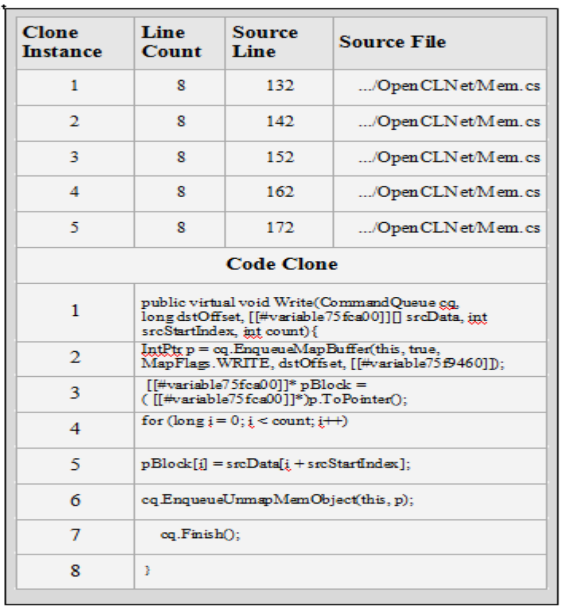
Meanings of the terms	
Meanings	Term
FC	File Count
TSLOC	Source Lines of Code
TCS	Total ColneSet

Table 3: Overall results obtained from the analysis of software



N.System	FC	SLOC	TCS
OpenCL.Net	50	10835	91
OpenPop.NET	71	14398	146
id3lib	254	38986	92
CANopen	83	14398	60

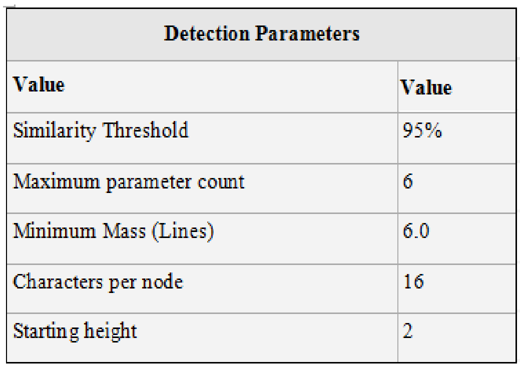
As mentioned in the previous section, there are several techniques to detect cloned code and each of these tools and techniques are introduced that can be used to detect cloned code. To perform this test, we have the tools CloneDr disposal. Figure 2 is an example of the code clone detection system software is OpenCLNet, according to Figure 5 to 8 lines of code clone "Mem.cs" is detected. The analysis was carried out; OpenPop file size of 71 and 140 clones that code has been detected. Id3lib with 254 files as well as 92 clones were identified code. 50 files as well as OpenCL code, we found 91 clones. The CANopen File 83 of 63 clones was found.



Clone Instance	Line Count	Source Line	Source File
1	8	132	.../OpenCLNet/Mem.cs
2	8	142	.../OpenCLNet/Mem.cs
3	8	152	.../OpenCLNet/Mem.cs
4	8	162	.../OpenCLNet/Mem.cs
5	8	172	.../OpenCLNet/Mem.cs
Code Clone			
1	public virtual void Write(CommandQueue cq, long dstOffset, [[#variable75fca00]][] srcData, int srcStartIndex, int count){		
2	IntPtr p = cq.EnqueueMapBuffer(this, true, MapFlags.WRITE, dstOffset, [[#variable75f9460]]);		
3	[[#variable75fca00]]* pBlock = ([[#variable75fca00]]*)p.ToPointer();		
4	for (long i = 0; i < count; i++)		
5	pBlock[i] = srcData[i + srcStartIndex];		
6	cq.EnqueueUnmapMemObject(this, p);		
7	cq.Finish();		
8	}		

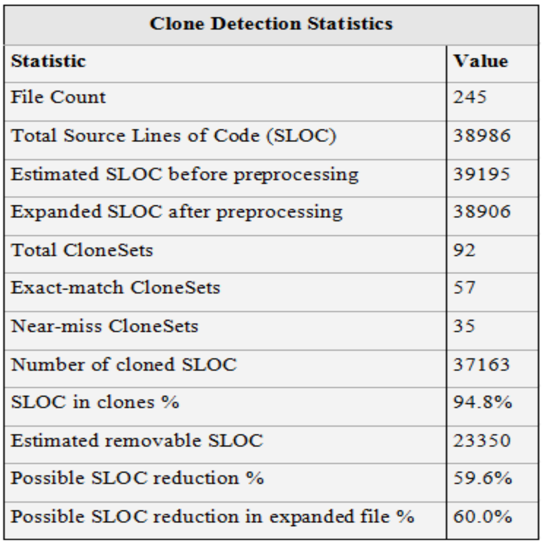
Figure 2: An example of an identified clone

Initial parameters of the instruments used for this analysis is shown in Figure 3 shows. The full results are shown in Figure 4 are obtained for the software (id3lib) are shown. Figure 5 also analyzed the results for the four open-source software, including the amount of code clones are detected and analyzed to show the number of files.



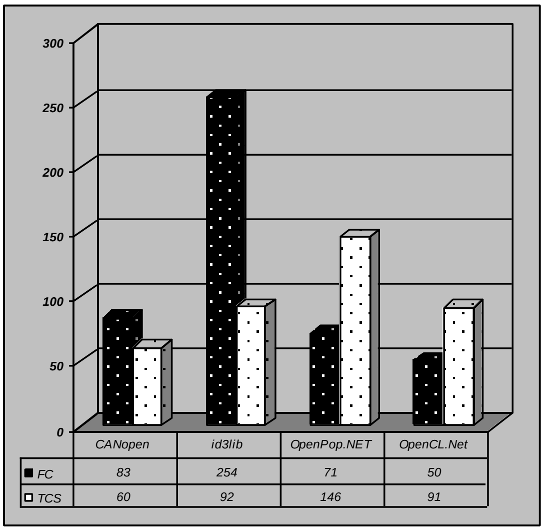
Detection Parameters	
Value	**Value**
Similarity Threshold	95%
Maximum parameter count	6
Minimum Mass (Lines)	6.0
Characters per node	16
Starting height	2

Figure 3. Initial parameters for analysis



Clone Detection Statistics	
Statistic	**Value**
File Count	245
Total Source Lines of Code (SLOC)	38986
Estimated SLOC before preprocessing	39195
Expanded SLOC after preprocessing	38906
Total CloneSets	92
Exact-match CloneSets	57
Near-miss CloneSets	35
Number of cloned SLOC	37163
SLOC in clones %	94.8%
Estimated removable SLOC	23350
Possible SLOC reduction %	59.6%
Possible SLOC reduction in expanded file %	60.0%

Figure 4. Results for id3lib



	CANopen	id3lib	OpenPop.NET	OpenCL.Net
■ FC	83	254	71	50
□ TCS	60	92	146	91

Figure 5. The overall results of the analysis of four open-source software

6 Conclusion

This paper deals with the code clone detection methods and some of the techniques and tools used to identify clones of code has been introduced and the case study analysis was a few open-source software systems to detect cloned code. The results of this study show that despite the immense complexity of the code clone detection in software systems, if there are common techniques used to clone overshadowed the quality of software code that can be attempted in order to identify clones. It is also hoped that the developers of software systems factors (such as quality programming) that creates a special attention should be cloned.

References

[1] K. Toshihiro, S. Kusumoto, and K. Inoue, "CCFinder: a multilinguistic token-based code clone detection system for large scale source code," *IEEE Transactions on Software Engineering*, vol. 28, no. 7, 2002.

[2] B. Elizabeth and J. Bailey, "Evaluating clone detection tools for use during preventative maintenance," in *2002 Proceedings of Second IEEE International Workshop on Source Code Analysis and Manipulation*, 2002.

[3] S. K. Ripon, et al., "Evaluating code clone genealogies at release level: An empirical study," in *2010 10th IEEE Working Conference on Source Code Analysis and Manipulation (SCAM)*, 2010.

[4] C. Fabio, F. Lanubile, and T. Mallardo, "Function clone detection in web applications: A semiautomated approach," *Journal of Web Engineering*, vol. 3, 2004.

[5] G. Panamoottil and N. Tsantalis, "Unification and refactoring of clones," *in CSMR-18/WCRE-21 Software Evolution Week*, 2014.

[6] U. Yasushi, et al., "Gemini: Maintenance support environment based on code clone analysis." *in Proceedings of Eighth IEEE Symposium on Software Metrics*, IEEE, 2002.

[7] M. Morshed, A. Rahman, S. U. Ahmed, "A literature review of code clone analysis to improve software maintenance process," arXiv preprint arXiv:1205.5615, 2012.

[8] S. Schulze, and D. Meyer. "On the robustness of clone detection to code obfuscation," *in 2013 7th International Workshop on Software Clones (IWSC)*, IEEE, 2013.

[9] B. S. Baker, "A program for identifying duplicated code," *in Proceedings of 24th Symposium on the Interface, Computing Science and Statistics*, vol. 24: 4957, Mar. 1992.

[10] M. Bruntink, "Aspect mining using clone class metrics," in 1st Workshop on Aspect Reverse Engineering, 2004.

[11] A. Agrawal, S. K. Yadav. "Technique for searching of similar code segments," International Journal of Soft Computing and Engineering, vol. 3, no. 1, Mar. 2013.

[12] M. Bruntink, A. van Deursen, R. van Engelen, and T. Tourwe, "An evaluation of clone detection techniques for identifying cross-cutting concerns," in Proc. International Conference on Software Maintenance, 2004.

[13] C. K. Roy, J. R. Cordy, "A survey on software clone detection research," Technical Report 541, Queen's University, Kingston, 2007.

[14] Y. Yuan, Y. Guo. "CMCD: Count matrix based code clone detection," *in 2011 18th Asia Pacific on Software Engineering Conference (APSEC)*, IEEE, 2011.

[15] http://www.semdesigns.com/Products/Clone/

[16] https://svn.ipd.kit.edu/trac/jplag/

[17] http://homepage.usask.ca/~mdu535/tools.html

Hamed Jelodar is received the B.Sc. degrees in computer software engineering from Islamic Azad University, Iran in 2012. He is a Master's student in Computer engineering and his research interests include Wireless Networks, Software Quality, Clone Detection, and Web Mining. Also, He has presented 5 papers in International Journal, 1 paper in International Conference and 4 papers in National Conference.

Javad Aramideh received his Master in Computer Engineering from Islamic Azad University, Sari, Iran in 2014 and his research interests include Wireless sensor Networks, ad-hoc network, Software Testing, Clone Detection, and Web Mining Also, He has presented 3 papers in International Journal, 1 paper in International Conference and 7 papers in National Conference.

Impact of Wormhole Attack on Data Aggregation in Hierarchical WSN

Mukesh Kumar and Kamlesh Dutta
(Corresponding author: Mukesh Kumar)

Department of Computer Science & Engineering
National Institute of Technology, Hamirpur(H.P.)-177005, India
(Email: mukeshk.chawla@gmail.com)

Abstract

Everyone uses wireless network for their convenience for transferring packets from one node to another without having a static infrastructure. In WSN, there are some nodes which are light weighted, small in size, having low computation overhead, and low cost known as sensor nodes. Sensors are only used to sense the data packet and transfer them to other nodes or base stations. They provide the bridge between users and base stations. There are some routing protocols available but they are not sufficient to detect the malicious node. We require a better security mechanisms or techniques to secure the network. Data aggregation is an essential paradigm in WSN. The idea is to combine data coming from different source nodes. In this paper, we give the brief introduction of WSN and data aggregation. Main focus is on wormhole attack and its countermeasures. We examine the impact of wormhole attack on data aggregation.

Keywords: Data Aggregation; Wireless Sensor Network; Wormhole Attack

1 Introduction

Wireless Sensor Networks (WSNs) generally consists of highly distributed network of small-size, lightweight wireless nodes. Wireless sensor network provides a bridge between the real physical and virtual world. Sensor network refers to the heterogeneous system which is primarily design for real-time collection. The sensors all together provide global views of the environments that offer more information than those local views provided by independently operating sensors. There are numerous potential applications of WSNs in various areas such as residence, industry, military, transportation, civil infrastructure, communication, security and many others. Elements of WSN are the base stations and the sensor nodes. Base station acts as a gateway between the wireless network and the external world. There are one or more several base stations in a network which can receive report from the sensor nodes, when they detect any event occurred in that network. Sensor nodes are used to monitor the physical or environmental attributes like temperature, humidity, pressure, sound, etc.

Among the designs of WSNs, security is one of the most important aspects that deserve great attention, considering the tremendous application opportunities [1].

In wireless networks, there is much more threat of attacks than in wired networks. The main characteristics of a WSN includes power consumption constraints, ability to cope with node failures, scalability of network, ability to withstand in harsh or disastrous environmental conditions, communication failures, etc. Security in sensor networks is complicated by the constrained capabilities of sensor node hardware and the properties of the deployment. The overall cost of the WSN should be as low as possible. The goal of security is to provide security services to defend against all the kinds of threats [3].

Data aggregation is basically a process in which we aggregate or combine the data and pass it to the aggregator node which is close to the sink node or base station in the network. In WSN, each node forwards data to its neighboring node which is nearer to the sink [16]. This scheme is not energy efficient. Therefore, we need a data aggregation approach. There are many approaches used in data aggregation. These are grid or centralized approach, cluster based approach, tree based approach, in-network based approach. Efficient data aggregation does not only provide energy constraint but also remove data redundancy and hence provide useful data only in the network. Even simple aggregation functions can easily be influenced by an attacker such that a network's behaviour can be altered (Wagner 2004) [16] with the help of sum, maximum, minimum, average function. These functions are insecure in data aggregation method. So we require security in these functions also or we can use them in some modified way.

There are two network in wireless sensor network i.e., flat and hierarchical network. In flat WSN, each sensor nodes has a same level to transmit the data. It uses the multi-hop path. The overhead is more but we get an optimal data. In hierarchical WSN, we consider a tree based topology in which root node act as a sink which takes all the aggregated data from the below level nodes and then transfer the data to above level of the tree. We need hierarchical WSN to get the energy efficiency and scalability. It involves data fusion at intermediate nodes; it reduces transmitted packets in the network. Results are propagated level by level in a tree. As we know, tree techniques or approach are not efficient in the network. If there is any failure of node then the entire setup is failed. Therefore, we combine both tree and cluster approach to get a new approach. It provides simple routing but not necessarily optimal routing. We focus on data aggregation in energy constraint sensor network. The main goal of data aggregation is to collect and aggregate all the data in an energy efficient manner so that the lifetime of the network is enhanced [14].

2 Literature Review

In wormhole attack, the adversary or the attacker carry packets, route, routing information, ACK, etc. through a link [6] to the legitimate node by making a tunnel between one adversary to other adversary and send packet to the legitimate node with a high speed then the original path or replays them in a different part. An attacker disrupts or intrudes forwarding messages that originated by senders, copies a portion or a whole packet and sending the copied packet through the tunnel [7] with a low latency so that it reaches before the original packet which traverses through the original route.

An attacker mostly situated near the base station, so it may easily interrupt the routing by creating a well placed wormhole [3]. Attacker convinces the legitimate nodes those have multiple hop from a base station, which are close to the wormhole. Sometimes it only copies the data of the packet and used as an eaves dropping attack. It can be used in the combination with the selective forwarding or eavesdropping [3]. Detection of wormhole attack is difficult when it conjucted with a sybil attack. Wormhole attacks are difficult to detect as they use a private out-of-band channel invisible to the underlying sensor network [3] by broadcasting in the network. Detecting wormhole attacks requires tight time synchronization among the nodes, which is infeasible in practical environment [6].

In Figure 1, we show the working of wormhole attack. In this, node H is an origin point of the packet. It sends the packet through G, F, E and then node C. Node C is the destination point of the legitimate node. Attacker interrupts the communication through the origin point to the destination point by copying a portion or a whole packet and sends that packet with a high speed through a tunnel, i.e., wormhole tunnel in such a way that the packet reaches the destination point before the original packet traverse through the original route.

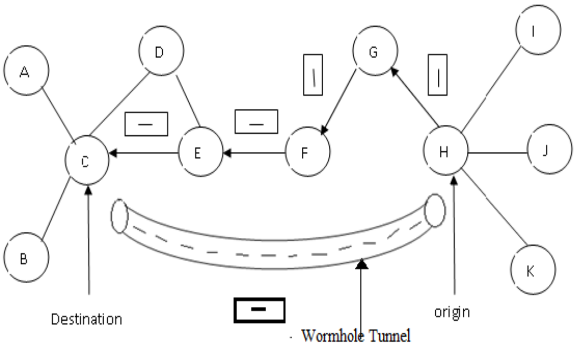


Figure1:Wormhole attack

Such a tunnel created by several means, i.e., by sending the copied packet through the wired network and at the end of transmitting over a wireless channel, using a boosting long distance antenna, sending through a low latency route or using any out-of-bound channel [5]. Wormhole attack is a harmful threat in the wireless sensor network, especially to routing protocols and it rely on geographic location and some attacks (e.g. selective forwarding, sinkhole, sybil, etc.) can be launched after wormhole attack [5].

3. Simulation

WiSeNet Simulator tool is used in the Wireless Sensor Network to developed or implement protocol and test them on a virtual WSN.
Test name: Wormhole attack
Description: We take 13 nodes to detect the attack by using the Gaussian Radio Model and Flooding node factory with a 130 radio range of a node.

Table 1: Countermeasures of wormhole attack

Schemes/ Techniques	**Description**	**Limitations/ Drawbacks**
Distance-bounding/ consistency based approach [8, 9]	This technique can be based on message travelling time information, directional antennas or geographical information	Requires additional and specialized hardware, therefore, it is inefficient in certain networks
Geographical Information-based Solutions [8]	The receiving packet compares the timing with the threshold value. The receiver has the knowledge of transmission distance and time.	Cannot detect exposed attacks because fake neighbors are created in exposed attacks
Localization-based solutions [8, 11]	Framework some nodes are determined as guard and uses GPS equipments. This technique is applied only on small network with limited resources or sensor nodes. Guard needs to know their own physical location with the help of GPS equipment.	If there is no packet loss in the network only then this method is applied.
Multi-dimensional Scaling-Visualization-Based Solutions [8]	Connectivity information and estimated distances are input to a multi-dimensional scaling (MDS) algorithm	Periodically monitors the visualization of nodes
Synchronized Clock-based Solutions [8]	Sensor nodes are tightly synchronized and each packet includes the time at which the packet is send. The receiver has the knowledge of transmission distance and time. If the transmission distance exceeds then it may be a wormhole attack.	Does not require special hardware but it cannot detect exposed attacks because fake neighbors are created in exposed attacks.
Secure Neighbor Discovery Approach [8]	The main idea is to monitor the network. Sensor nodes build the neighboring list and determine the traffic going in and out of its neighbors. This technique is working as ranging, exchanging and making neighbor tables and verifies the neighbors.	Less accuracy and unavailability of resource s.
Trust-based Solutions [8]	Sensor nodes monitor their neighboring nodes and rate them which are used in a trust based system. If the node behaves differently then we consider it as a malicious node. It combines time-based and trust-based module to detect the sensor nodes that sends the false data in the network. These two systems run in parallel.	Costly.

3.1 Test Conditions

Table 2 shows the test conditions. These are the condition set to test the virtual network. We initialize total Number of nodes are 13, sender nodes are 6, receiver nodes are 5 and 2 attacked nodes.

Table 2: Test conditions

Total No. of Nodes	**13**	**50**	**101**
No. of Stable Nodes	13	50	101
No. of Sender Nodes	6	47	98
No. of Receiver Nodes	5	1	1
No. of Attacked Nodes	2	2	2
Average Neighbour p/node- radio	9	15	21
No. of Messages Sent	30	94	196
No. of Messages Received	30	0	0
No. of Messages Attacked	30	94	196

3.2 Transmission Rate

Table 3 shows the transmission rate of messages. It tells about the transmission and retransmission rate of message send.

Table 3: Transmission rate

Send message	0
Message/rate	0
Sends with 0 retransmission	

3.3 Topology

In Figure 2, we show a topology of 12 nodes which are interconnected to each other and only 1 node is connected to sink node(base station). This shows that the data aggregations in which only 1 node send/receive all the data to/from the base station of the network.

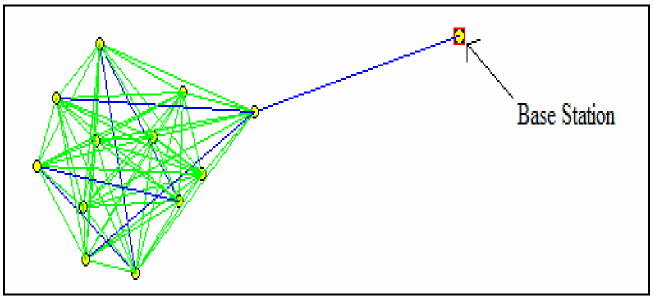


Figure 2: Topology of 12 nodes and 1 sink node (base station)

3.4 Topology After Assigning Nodes

In Figure 3, there are 13 nodes in which 2 adversary nodes, 5 receiver nodes and 6 sender nodes (including base station node).

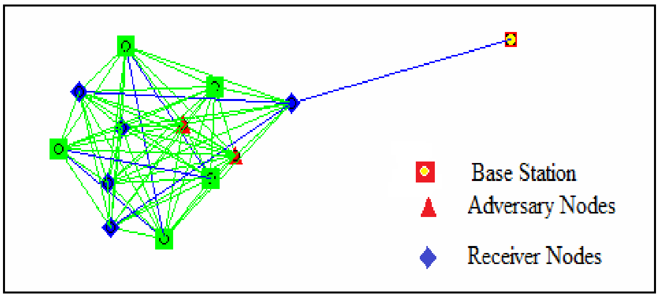


Figure 3: Topology after assigning adversary, sender and receiver nodes (13 nodes)

In Figure 4, there are 50 nodes in which 2 adversary nodes, 1 receiver nodes and 47 sender nodes (including base station node).

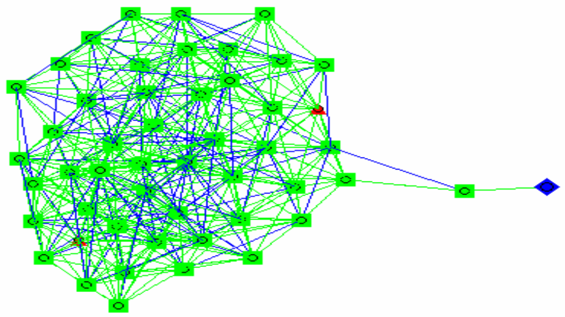


Figure 4: Topology after assigning adversary, sender and receiver nodes (50 nodes)

In Figure 5, there are 101 nodes in which 2 adversary nodes, 1 receiver nodes and 98 sender nodes (including base station node).

4. Results

We get the result by observing parameters i.e., reliability, coverage, latency and energy. These are the main parameters which are given by WiSeNet Simulation Tool as a result.

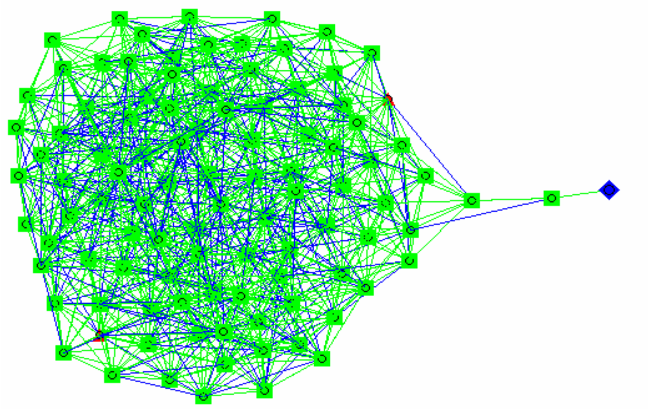


Figure 5: Topology after assigning adversary, sender and receiver nodes (101 nodes)

4.1 Reliability

Reliability refers to proper transmission of messages in the network. Each and every message which is sent to nodes would be received by receiver nodes otherwise retransmission should apply. Table 4 shows the reliability of 100%.

Table 4: Reliability

Total No. of Nodes	**13**	**50**	**101**
Total Message Sent	30	94	196
Total Message Received	30	93	195
Reliability %	100	98.0	99.0

4.2 Coverage

Coverage refers to all the nodes are covered in the topology. Table 5 shows the coverage of nodes which gives 100% reliability in this example.

Table 5: Coverage

Total No. of Nodes	**13**	**50**	**101**
No. of Sender Nodes	6	47	98
No. of Covered Nodes	6	47	98
Coverage %	100.0	100.0	100.0

4.3 Latency

It means if there is more number of attackers present then there is more delay of the message received by the nodes. Table 6 shows the latency of the message, average latency is $2.\overline{3}$.

Table 6: Latency

Total No. of Nodes	**13**	**50**	**101**
Maximum	3.0	9.0	10.0
Minimum	2.0	1.0	1.0
Average	2.233333333333333	5.28723404255	6.23979591836

4.4 Energy

It shows the consumption of energy by per node. Table 7 shows the total consumption of energy and average consumption by per node in that topology.

Table 7: Total and average consumption of energy

Total No. of Nodes	**13**	**50**	**101**
Average Consumption p/node(J)	0.007923418923076929	0.028792674119999924	0.06417608158415736
Total Energy Consumption (J)	0.10300444599999949	1.4396337060003304	6.481784240007351

4.5 Simulation Energy

In Table 8, we show the energy model parameters which are concerned at the time of simulation. Each and every energy parameters have their own values. Energy consumption by protocol event and phases: There are two charts of energy consumption by protocol.

Table 8: Energy model parameters

Parameter	**Value**
Sign Energy (Joules/Byte)	0.0000059
Total Energy (Joules)	9360
CPU Transition to ON Energy (Joules)	0.000000001
Sleep State Energy (Joules)	0.0000075
Idle State Energy (Joules)	0.0000059
Transceiver Transition to ON Energy	0.000000002
Encrypt Energy (Joules/Byte)	0.000001788
Verify Digest Energy (Joules/Byte)	0.0000059
Reception Energy (Joules/Byte)	0.0000286
Verify Signature Energy (Joules/Byte)	0.0000059
Digest Energy(Joules/Byte)	0.0000059
Simple Processing Energy (Joules)	0.0138
Decrypt Energy (Joules/Byte)	0.000001788

In Table 9, we show the energy consumption by protocol by considering 3 types of topology that contain 13 nodes, 50 nodes and 101 nodes.

Table 9: Energy consumption by protocol

Total No. of Nodes	**13**	**50**	**101**
Energy Consumption by Protocol Event			
TxTransitionToON	(0)0%	(0)0%	(0)0%
Receiving	(0.027)26%	(0.398)28%	(1.962)30%
Transmission	(0.076)74%	(1.041)72%	(4.52)70%
Energy Consumption by Protocol Phases			
NOPHASE_DEFINED	(0.103)100%	(1.44) 100%	(6.482)100%

In Figure 6, we have shown that with increase in number of nodes in network the energy consumption of protocol is increases.

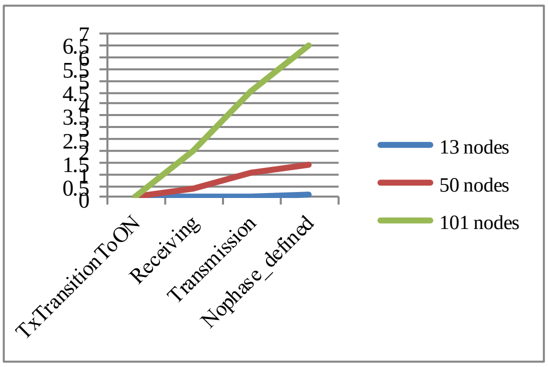


Figure 6: Energy consumption by various number of nodes

5. Conclusion and Future Scope

A sensor network contains one or more sinks in which all the data is collected or transmitted. Sensors act as a source in the network which sense the event and push back the relevant data in the environment. Data aggregation is an essential paradigm for wireless routing in the network. Data aggregation is usually defines as to collect and gather the data from multiple sensors at intermediate nodes, aggregate the data and then transmit the data to the base station or sink. The main focus of data aggregation is to get efficient organization, routing and data aggregation approaches to construct the topologies. In simulation result, sensor network which using data aggregation has low energy consumption, data latency, redundancy and increased reliability. Future work will focuses on the detection and prevention of network through wormhole attack by using data aggregation technique. This type of topology has many difficulties. We would extend our research to detect wormhole attack and secure the network. Security is the main issue in data aggregation. We have to secure the network by using integrating security in data aggregation. A number of challenges present in that area of secure data aggregation for sensor network and it is worth exploring in the future.

References

[1] G. Padmavathi, D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *International Journal of Computer Science And Information Security*, vol. 4, no. 1 & 2, 2009.

[2] Z. Feng, G. Leonidas, Wireless Sensor Networks, *Morgan Kaufmann Publications*, 2004.

[3] H. C. Chaudhari, L. U. Kadam, "Wireless sensor networks: security, attacks and challenges," *International Journal of Networking*, vol. 1, no. 1, pp. 04-16, 2011.

[4] S. Dharmendra, M. R. Ahmed, X. Huang, "A taxonomy of internal attacks in wireless sensor network," *World Academy of Science, Engineering and Technology*, 2012.

[5] G. Murugaboopathi, J. Murugaboopathi, K. Venkatatraman, "Various attacks in wireless sensor network: survey," *International Journal of Soft Computing and Engineering*, vol. 3, no. 1, 2013.

[6] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *in First IEEE International Workshop on Sensor Network Protocols and Applications*, 2003.

[7] G. Inan, M. Meghdadi, S. Ozdemir, "A survey of wormhole-based attacks and their countermeasures in wireless sensor networks," *IEEE Technical Review*, vol. 28, no. 2, pp. 94-98. 2011.

[8] S. Brands, D. Chaum, "Distance-bounding protocols," *in Eurocrypt'93*, LNCS 765, pp. 344-59. 1994.

[9] J. P. Hubaux, L. S. Buttyan, "SECTOR: Secure tracking of node encounters in multi-hop wireless networks," *in Proceeding of the first ACM Workshop on Security of Ad-Hoc and Sensor Networks (SANS 03)*, pp. 21-32, 2003.

[10] W. Bo, G. Fuxiang, Y. Lan, D. Xiaomei, Z. Zhibin, "Detecting wormhole attacks in wireless sensor networks with statistical analysis," *in International Conference on Information Engineering*, 2010.

[11] T. Giannetsos, T. Dimitriou, N. R. Prasad, "State of the art on defences against wormhole attacks in wireless sensor networks", *in 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology*, pp. 313-318, 2009.

[12] R. Rajagopalan, P. K. Varshney, "Data aggregation techniques in sensor networks: A survey," *Communications surveys and tutorials, IEEE*, vol. 8, no. 4, pp. 48-63, 2006

[13] B. Krishnamachari, D. Estrin, S. Wicker, "The impact of data aggregation in wireless sensor networks," *in Proceeding 22nd International Conference on Distributed Computing Systems Workshops*, 2002.

[14] N. S. Patil, P. R. Patil, "Data aggregation in wireless sensor network," *in IEEE International Conference on Computational Intellegence and Computing Research*, 2010.

[15] D. Waltenegus, P. Christian, Fundamentals of Wireless Sensor Network: Theory and Practice in a John Wiley and Sons, Ltd., Publication, 2010.

Mukesh Kumar is Associate Professor in the Department of Computer Science & Engineering at Echelon Institute of Technology, Faridabad (Haryana) INDIA. He received his B. Tech in Computer Engineering from Kurkshetra University, Kurkshetra, INDIA in 2004 and M. Tech in Computer Science & Engineering from NIT, Hamirpur. (H.P.) India in 2009. Presently he is doing Ph.D. in CSE from Department of CSE, NIT Hamirpur (H.P.) India. He has more than 9 years of experience in teaching and research. His area of research is mobile computing, computer networks and network security. He has published more than 15 research papers in various international journals and conferences. He is acting as Branch Counselor of IEEE Student Branch of the institution. He is a professional member of IEEE, life member of ISOC, and life member of IAENG.

Kamlesh Dutta is Associate Professor in the Department of Computer Science & Engineering at National Institute of Technology, Hamirpur (Himachal Pradesh) INDIA. She is working in the faculty CSE Department, NIT Hamirpur since 1991. Before that, for two years she has served in Banasthali Vidyapeeth, Rajasthan. She obtained her PhD from Guru Gobind Singh Indraprastha University (Delhi) INDIA, MTech from Indian Institute of Technology, Delhi and MS from

Vladimir State University, Russia. Her major research interests include Network Security, Software Engineering and Artificial Intelligence. She continues to mentor several undergraduate and postgraduate students in these areas. Several students are working under her guidance toward MTech/PhD. Dr. Dutta held the charge of coordinator, Video conferencing from 2006 to 2011, Coordinator Communication (2008-2011) and coordinator Institute Library (2006-2008). Presently, she is the chairman of library automation committee. Dr. Dutta is actively engaged in the organization of short term training programs, workshops, seminars and conferences. She has delivered technical talks on various topics. She is in the national and international committees of various international conferences and Journals. She is the lifetime member of ISTE, SIGSEM and SIGDIAL. Her papers appeared in International Academic Journals and conferences such as ACM, IEEE, Springer, Elsevier etc. Dr. Dutta visited Singapore and Australia regarding training under UNDP and Cisco. She visited several universities during her abroad visits for paper presentation, training etc. Dr. Dutta received outstanding award for her contribution to the Cisco Networking Academy Program in 2001, best paper award for the paper titled “Adoption of Video Conferencing in Technical Institutions-a Case Study of NIT Hamirpur”, in ISTE Section Annual Convention 2007.

Isha Chopra is working as Assistant Professor in the Department of CSE, Echelon Institute of Technology, Faridabad, INDIA. She has done her B. Tech and M. Tech from M.D.U., Rohtak, INDIA.

Cyber-Attacks in Cloud Computing: A Case Study

Jitendra Singh

Department of Computer Science, PGDAV College, University of Delhi
Ring Road, Nehru Nagar, New Delhi, India, PIN-110065, India
(Email: jitendra.singh0705@gmail.com)

(Received June 6, 2014; revised and accepted Aug. 17, 2014)

Abstract

Cloud computing has emerged from the legacy system; consequently, threats applicable in legacy system are equally applicable to cloud computing. In addition, cloud specific new threats have also emerged due to the various reasons including, multi-tenancy, access from anywhere, control of cloud, etc. Considering the significance of cloud security, this work is an attempt to identify the major threat factors to cloud security that may be critical in cloud environment. It also highlights the various methods employed by the attackers to cause the damage. To accomplish our objective, we have reviewed the major publication related to cyber security. It is revealed that cyber-attacks are industry specific and vary significantly from one industry type to another. Finally, we have conducted the case study on cyber-attacks that are already occurred in cloud paradigm. Cyber-attacks were highlighted by categorizing them into phishing attacks and distributed denial of services. This work will be profoundly helpful to the industry and researchers in understanding the various cloud specific cyber-attack and enable them to evolve the strategy to counter them more effectively.

Keywords: Cyber security, cloud Attack, cybercrime, resource protection, cloud threat

1 Introduction

Enterprises and individual users prefer outsourcing their services on the web, instead of maintaining the resources of their own. Outsourcing of technical resources enables the organization to concentrate on business need instead of technical aspect that is managed by the experts in Information Technology (IT) area. To facilitate such users, a web based paradigm known as cloud computing has emerged and offering the services on utility model [13]. The major goal of Cloud computing is to reduce the operating cost, increase throughput, increase the reliability and availability [12].

To cater the need of wide variety of users, cloud is offering three types of services. These services include Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [17]. In IaaS, users are offered the computing capabilities such as processor, RAM, Storage, etc. as Services [4]. All these resources are offered on rent basis from the cloud instead of private services [9]. The appealing feature of the IaaS is that the users do not need to change the infrastructure periodically, which gets outdated in every three years due to the Murphy’s Law. Users are also free from updating the operating system, installing the new patches that are frequently needed to plug the exploited vulnerabilities.

In PaaS, development environment is offered as a service; whereas in SaaS, applications are offered as services. In SaaS environment, applications subscribed are available for use without any delay, while in legacy system user has to wait for months or sometimes for years to get the application developed. Google docs, invoices, cloud ERP, etc. is some of the prominent examples of SaaS based services. All the cloud services (IaaS, PaaS, and SaaS) are offered via public, private or community based deployment model. All these cloud deployment models have been classified depending upon the ownership held by the cloud user. If the cloud resources are under the control of cloud users, then it is known as private model (aka on-premises model), whereas if the cloud resources are under the control of cloud provider in that case it is known as public cloud (aka hosted model). In public model, resources are accessed with the help of software known as clients that connect to the cloud server remotely. Desktop, Laptop, Smartphones, etc. are some of the clients that can be utilized to access the cloud resources.

Despite of the above advantages, Cloud computing has also lead to the emergence of various challenges. Various factors need to be considered before the cloud adoption. Many of these issues are attributed due to the remote availability of resources, location of data center in other country, no control on data center, etc. All the above issues pave the fertile ground to the cyber attacker to determine the vulnerabilities and exploit the cloud resources. Many of the authors have considered security as the major challenge [6, 13].

2 Security in Cloud Computing

Security in the cloud computing is a major challenge and retarding the proliferation of cloud computing [8, 19, 28]. Understanding the criticality involved in cloud security, various working groups and standard organizations have been formed to take up cloud security. Cloud security alliance (CSA), NIST, ENISA, etc. are some of the prominent groups working for the cloud security and suggesting their recommendations, releasing the guidelines, to secure the cloud. Among all the above groups, Cloud security alliance is entirely committed for the cloud security. Many of the significant documents have already been published by CSA related to the cloud security.

To identify the major contemporary threats, CSA has published the report on the top threats. Although, similar report was also published earlier in 2010 titling 'Top Threats to Cloud Computing V1.0' [8], but the new study was required due to the change in methodologies by the attackers and to examine the current security trend in cloud computing. The report is published with the title 'The Notorious Nine Cloud Computing Top Threats in 2013' [7]. In this study, CSA has reviewed thousands of article related to cloud threat, asked from a number of experts and visited the different website. Correspondingly, the group has identified the major threats on cloud computing that have significant impact in cloud computing. In this most recent report, experts have identified the following nine critical threats to cloud security (ranked in order of severity):

1). Data Breaches

2). Data Loss

3). Account Hijacking

4). Insecure APIs

5). Denial of Service

6). Malicious Insiders

7). Abuse of Cloud Services

8). Insufficient Due Diligence

9). Shared Technology Issues.

2.1 Data Breaches and Data Loss

Once the information is available to any entity, other than the owner then it is known as data breach. It is more critical in cloud computing where the data is under the control of third party and promotes the resource sharing among many users. Cloud computing has also opened the new avenue of attacks including side channel attack. In this attack, the adversary can use virtual machine's side channel timing information to extract the private cryptographic key used in other's VM on the same physical server. Multi-tenancy architecture of cloud computing also offers more vulnerability, if it is not properly designed. Flaw exist in one user's database can affect the safety and security of others data stored in the same cloud.

Data loss is the other key issue related to cloud security. In data loss users are losing the information stored, whereas in data breaches, information is stolen by the adversaries. For instance to secure the data, user may opt for data security. But loss in encryption key may result in data loss. Similarly, to prevent the catastrophic loss if the user is storing the data in backup devices, it means data is more vulnerable to attack. Data breaches is applicable in IaaS, PaaS and SaaS deployment model of the cloud computing. It is believed that this threat is still relevant.

2.2 Account Hijacking and Denial of Service

Account hijacking exists in legacy system, where adversary takes over the control of user's account. In cloud paradigm it poses additional challenges. For instance, if credential is stolen by the adversary then he can eves drop, modify, information even worst can direct cloud users to illegitimate web site. In the denial of services, illegitimate users are using the cloud resources and denying the legitimate users from accessing the resources. In cloud computing distributed denial of services (DDoS) attacks are frequently caused.

2.3 Insecure APIs

Cloud providers are offering their API's to the developers so that they can develop the application to connect to their cloud. These API's are openly available and can easily be used by the developer community. But it has been observed that the API's that are offered are not secured enough, as needed for the cloud environment. This vulnerability has been observed due to third party usage of cloud APIs. Consequently, insecure API's make the cloud vulnerable to various attacks.

2.4 Abuse of Cloud Services and Malicious Insider

Cloud providers maintain the huge resources. Once the cloud users subscribe for the cloud resources they are passed under the control of subscribed users. This subscriber may be an adversary. Consequently, huge resources come under the disposal of adversary that can be utilized by him in various analyses. In legacy system, to buy such resources required huge investment, consequently huge computation was not possible.

User's rights are given to perform certain task for the smooth functioning of the organization. However, it has been observed that these services are mis-utilized, particularly by the power user, for instance System administrator.

The other major threat is malicious insider, in which someone from the inside only facilitates in external attacks. These passages may be provided intentionally or un-intentionally. Opening of the mail that has received by the user and clicking the link provided aims of knowing more about the users organization falls under the category of un-intentional attack.

2.5 Undue Diligence, Selection for Cloud Selection

Many of the users are selecting the cloud due to huge infrastructure, minimum upfront cost, security offered by the cloud, etc. Considering the huge potential growth many new cloud provider have emerged and continue to emerge on daily basis. Consequently, it is imperative to conduct the sufficient background check of the cloud provider, security offered, regulatory compliance, etc. used by them. Necessary contract related to data availability is also need to be placed to avoid any future disputes.

2.6 Shared Technology Usage

In the IaaS model of cloud, resources such as processor, memory, bandwidth etc. are utilized by the subscribers on shared basis. Similarly, in SaaS environment, same application is shared among many users. In cloud, Hypervisor have significant role in isolation and resource provisioning. Since, all the users are on the top layer of hypervisor, if the security of the hypervisor is compromised, security of the entire cloud may be breached at once.

3 Study on Cyber-Attack in Cloud Computing

Cloud resources are the attractive ground for the cyber-criminals due to the huge resources available at the centralized place. Accessibility by anyone subscribing, and from anywhere is highly suitable for cyber criminals. Now, they can access the resources from any part of the world and any time, even the use of device is not restricting the usage of cloud resources. Consequently, huge cloud resources under the disposal of adversary pose major threats to the cloud and web users. They are utilizing cloud resources in many of their cyber-attacks.

McAfee and Guardian analytics have uncovered sophisticated attack that are targeting to financial services. Before, it was considered that cyber-crime is confined to the Europe but the study revealed that it is reached to other parts of the world, including US and Columbia. These attacks are automated and targeting the account with huge balance. In addition, they have also targeted the credit union, large global bank, and regional bank. From these fraudulent activities they could manage to transfer $78 million (USD) from various accounts of Financial Institutions.

3.1 Review of Cloud Threats

Being a new paradigm and concentration of resources, there is great threat to cloud computing. Twelve major threats have been identified by the [11]. Identified threats have been denoted as T1 to T12. Abuse and nefarious use of cloud has been named as T1, insecure interfaces as T2, malicious insiders as T3, etc. Other threats and their nomenclature have discussed in Table 1.

Critically of these threats can be identified with the number of attacks that have already taken place. As per the study conducted by [1], T2 (Insecure interfaces and APIs) have been considered as the major threat, it is followed by T5 (Data loss or leakage). Ranking of other threats can be determined by Figure 1 [11].

Table 1: Threats in cloud computing

Abuse and Nefarious Use of Cloud Computing	Insecure Interfaces and APIs	Malicious Insiders	Shared Technology Issues	Data Loss or Leakage	Account or Service Hijacking
T1	T2	T3	T4	T5	T6
Unknown Risk Profile	Cloud related malware	Natural Disaster	Closure of cloud services	Cloud related malware	Inadequate Infrastructure Design and Planning
T7	T8	T9	T10	T11	T12

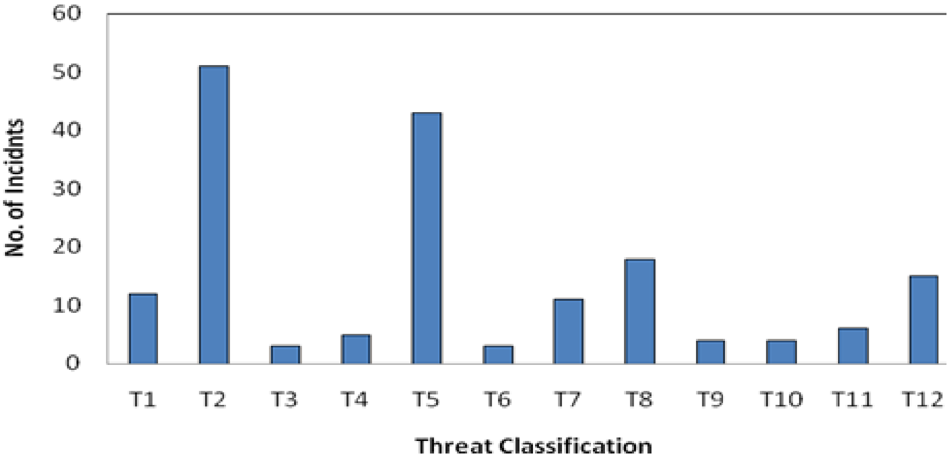


Figure 1: Threat classification

Once we further drilled down to identify which cloud is most affected (determined by the number of incidents that took place), while comparing to other clouds big cloud giant’s (Google, Amazon, Microsoft etc.) are primarily targeted by the cyber criminals. Number of incidents that took place in different cloud has been illustrated in Figure 2.

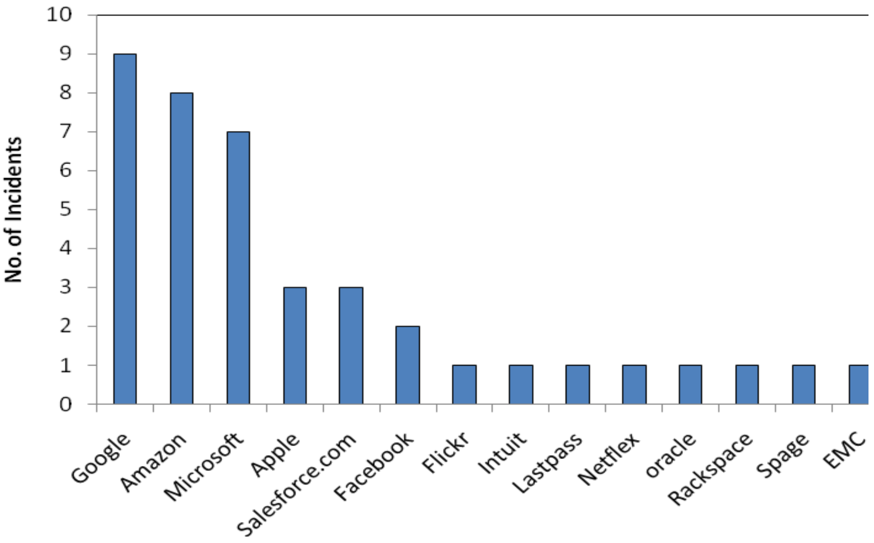


Figure 2: Number of incidents reported in major cloud

3.2 Study on the Type of Industry Targeted

Recently, IBM security services, 'cyber security intelligence index has carried out the study to figure out the industry that is most attacked by cyber criminals. As per this study, finance and infrastructure, ICT, & health and social services are the prominent industry types that are attracting to cyber-criminal in huge number. From the total cyber-attack that took place 20.9% were directed to finance and insurance domain.

Majority of the attacks are caused by the outsiders and consisting of 50% of the total attackers [15]. However, malicious insiders are equally a cause of cyber-attack, and causing 20% of the overall attack. The key objectives of these attacks were to harm the ICT users in one way or the other and the same has been illustrated in the Figure 3 [1].

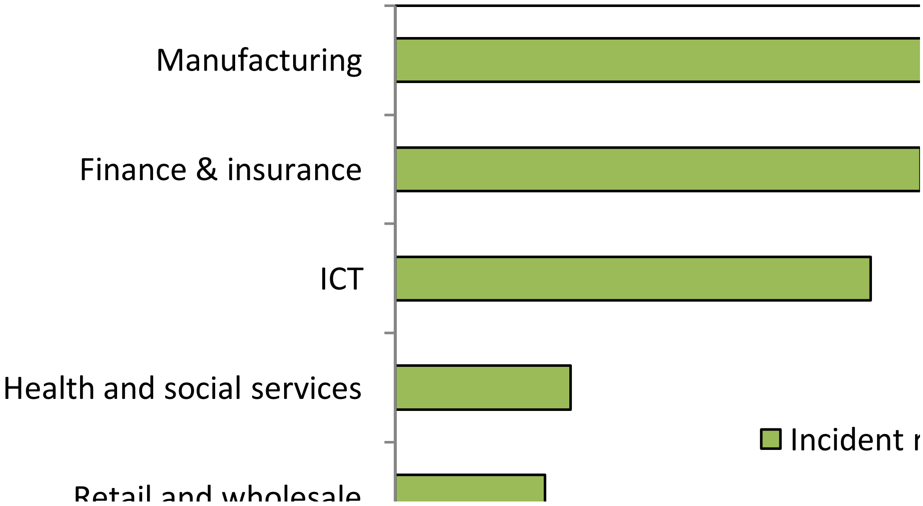


Figure 3: Attack incident rates as per the industry (Source: [15])

3.3 Categories of Cyber-Attack in Cloud

As per the study conducted by AlertLogic on its customer, it was observed that more than 45,000 security incidents were verified between 01April 2012 to 30 Sept 2012 [1]. In this study, cloud computing was categorized into hosted cloud and enterprise data center. Hosted model is similar to public model where the resources are under the control of cloud provider. The other model (enterprise model) is privately owned model where the resources are under the control of the owner. Study revealed that hosted cloud security is better than the enterprise data center. Cyber-attacks that are taking place in hosted data center and enterprises data center are not same [1]. However, for our study we have considered the common factors that are applicable in both the model to compare them which is more secure.

Study has considered the incidents which are caused by malware/botnet, Brute force attack, and web app attack in hosted and enterprise model. Incidents along with their definition have been depicted in Table 2.

Table 2: Incident descriptions and their definitions

S.No.	Incident Descriptions	Definitions
1.	Malware/botnet	Malicious software deployed on a host and gets involved in unscrupulous activities, such as data destruction, information gathering or creation of backdoors.
2.	Brute force	Exploit attempts enumerating a large number of combinations typically involving multiple credential failures, in hopes of finding a weak door.
3.	Web app Attack	Attacks targeting the presentation, logic or database layer of web apps

As per the Alertlogic's study, Enterprise data center are much affected with the Malware activities that account to 49%, and followed by Brute force attack with 49%. Whereas, it is less frequent in hosted model [1]. Same is also illustrated in Figure 4 [1]. In hosted model, web application attacks are more relative to the enterprise model and account for 52% of the total attack [1]. Majority of these attacks are taking place with automated software.

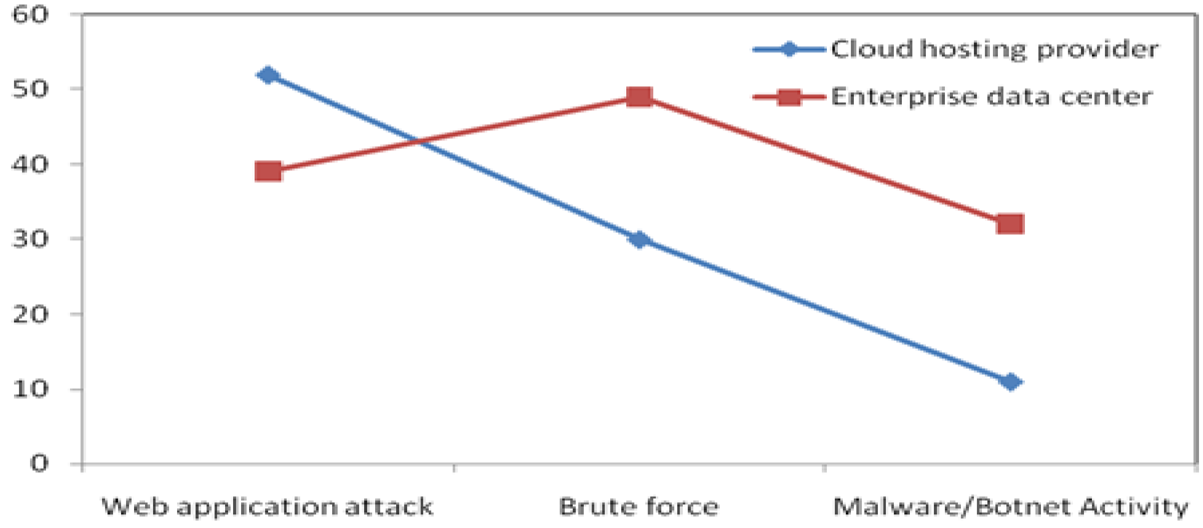


Figure 4: Categories of attack on hosted and enterprise data center

With the help of Figure 4, it can be concluded that hosted model of cloud is more secure relative to the enterprise model when we consider brute force attack or the malware/botnet attack. However, web application attacks are more in hosted model of cloud in comparison to the enterprise model.

4 A Case Study on Cyber-Attacks in Cloud

Information security is all about Confidentiality, Integrity & availability (CIA) [6]. Among the CIA, administration are more focused on confidentiality and integrity due to the involvement of regulatory compliances. Lack of focus on availability makes it more vulnerable to attacks. Recent attacks that took place in cloud are the examples of security hole exploited by cyber-criminals. Cyber attackers resort the cloud and leveraging it various platforms for malware infection and data ex-filtration. DBaaS is one of the services that are attacked by the cyber-crime [13]. This is revealed by the recent study titling 'Assessing the threat of DBaaS landscape' carried out by security outfit Imperva to analyze how the DBaaS is affected by the cyber criminals.

4.1 Identifying the Major Factors of Cyber Crime

To study the major breaches in cyberspace particularly cloud computing, we have identified the factors that can have significant impact on cloud security. To attain this objective, we have reviewed the literature published in prominent research journals. Further, we have also reviewed the publications from the varieties of working groups active in this domain including cloud security alliance, ENISA, NIST, etc. Survey and findings of security organizations, for instance Kaspersky, Micro-trend, and McAfee has been extensively reviewed.

By reviewing the literature [3, 6, 13, 21, 22, 27] it is revealed that DDoS is the major threat in cloud computing and need to be addressed at appropriate level. In DDoS, legitimate users are denied the resources due to the excessive use by non-legitimate users [21, 29]. Further identified the other characteristics of DDoS attack and revealed that average DDoS exist for 19 hours. It further highlights that 28% of the threats generate from the US while 35% from china. [2] Released the demographic report on how the Denial of services effecting the users globally. Whereas [6, 15, 23, 24, 25] have identified phishing as major threat. Study reveals that major frauds are taking place due to the phishing attacks and same is growing at phenomenal rate. Spear phishing is also an appealing method to the cyber attackers for attacking the various users reveals ThreatSim.

From the above review it is concluded that DDoS and Phishing are the major threats and need extensive study for their occurrences and damage caused.

4.2 Phishing Attacks in Cloud

In the phishing attacks, users are working on a fraudulent side that appears to be legitimate site. Phishing sites are created to obtain the users credential. The other phishing attack is through the e-mail, where users received the e-mail from the adversaries. E-mail received appears as legitimate mail from the known source. Such mails provide very concise or no information and provides the link to know more about it. Once clicked on the embedded link sent, malware gets installed on the user's PC. A number of phishing attacks have already occurred in the cloud. Some of them have been discussed in the upcoming sub-section.

4.2.1 Longline Phishing

Longline phishing is a new type of attack that is occurring in the cloud. In this type of attack, adversaries take the advantage of email services and sought the personal information from the users. Attackers sent the mail to the cloud user tricking him to click the link [18].

4.2.2 Spear Phish Attack on Raythe

Defense company Raythe have also encountered the phishing attack in its cloud. It was a spear phishing attack, an email was sent to the employees to access an application through this e-mail link. However no damage was reported due to the outgoing filters that were in place.

4.2.3 Phishing Attack on Microsoft Employees

Recently, some of the phishing attacks occurred on the account of Microsoft employee that was maintained on social media and emails [11]. These accounts were targeted phishing attack. It occurred to obtained the law enforcement information inquiries.

4.2.4 Phishing Attack on Dropbox

Phishing attack is also uncovered in Dropbox users account by the security firm Appriver [10]. This attack phishes victim's password via bogus email once succeeded then users computers are infected with malware. They send an official appearing mail to reset the password once clicked by the user on the reset button a malware gets installed on the user's browser.

4.2.5 Phishing Attack on South Carolina

Another major phishing attack observed at South Carolina [26]. The data breaches have stolen millions of social security numbers, bank account information and thousands of credit card and debit card information. When investigated, it is uncovered that at least one of the employees has clicked on the embedded link containing the malware. However, the source from where attacker received the employee's credential remained unknown. Attacker were not confined themselves with this attack only, instead gained the access of more system and deployed the malware on them to get more credentials.

4.2.6 Phishing Attack on Amazon and Apple

One of the major data breach occurred with Apple and Amazon [18]. In this breach, Honan's accounts on Apple and Amazon were compromised. In these attacks, victim has lost all his information stored in his account. Additionally, he has lost the photo and video of his 18 years daughter, which he has not stored anywhere else.

4.2.7 Phishing Attack on DBaaS

Recent trend is to offer database as a Service. In this model user can subscribe for the relational database to leverage this cloud offering. Amazon and Microsoft both are offering DBaaS. Users can benefit by these services by subscribing to it and pay for its usage.

But a recent report by Imperva highlights that DBaaS is extremely risky and can be exploited by Command and Control (C & C) Server, if necessary precautions are not observed [16]. To examine the vulnerabilities, [16] conducted the research and concluded that cloud subscription is fairly risky due to the fact that same database can be shared/ subscribed by the adversaries. This will result in easy access and attack on database. To support their claim they have carried out a research that revealed that mail sent to a user may lead to execute the malware in his system and connect the users system to remote location that is controlled by the adversaries. OLEDB provides the necessary connectivity to connect the database. In addition, report revealed that vulnerabilities existing in the database provide further ground to attack DBaaS.

4.3 DDoS Attack in Cloud Computing

Distributed denial of services is the other category of prominent cyber-attack that is taking place in cloud computing. Distributed denial of services attack is the cyber-attack in which a number of computers are used to attack the single destination. Compromised computer are known as Zombie. Due to DDoS, legitimate users are denied the resources, since they are utilized by non-legitimate users.

DDoS exploit the volumetric technique or the amplification technique. In the volumetric technique huge volume of traffic is directed to the network in order to consume the bandwidth or resource-sapping exhausts. State exhaustion attacks such as TCP SYN flood, and idle session attacks are the example of misuse of state nature of TCP and causes the resource exhaustion.

In the amplification technique, attackers take the help of victim to increase the traffic. An amplification technique, attacker exploits the attacked resource. Attacked botnet send out a DNS query of about 60 bytes to an open recursive DNS resolver that respond with response message up to 400 bytes, increasing the amount of traffic by more than the factor of 60.

Upcoming sub-section discussed the major DDoS attacks that have already been caused.

4.3.1 Attack on Spamhous

Spamhous is a spam avoiding company. Recently, DDoS attack took place in spamhous project [20]. The attack exploited the DNS Servers, open DNS resolver's capability. In this attack, peak attack traffic has reached to the capacity of the server. The peak attack traffic has reached to the volume of 300 gigabit per second. To handle the issue spamhous released a press note advising the internet community to check the traffic leaving their network to stop spoofed sending addresses is not leaving their network and to lock down any open DNS resolver [20].

4.3.2 Security Breach in Sony

Security breach on Sony has alerted the whole internet community [5]. Attack has exposed 100 million account records. Attackers not remained concentrated on this attack instead an additional attack occurred on Sony's online entertainment that exposed additional 25 million users. To determine the reasons, company constituted an investigation team. It was revealed that attack took place due to the availability of two servers behind the firewall. The two servers were web server and the application servers. Attacker exploited the vulnerabilities of application servers and attacked the web Server [5].

4.3.3 DDoS Attack Took Place on Bitbuchet

Bitbuchet is a development company that hosted it's infrastructure on cloud. It has subscribed to Amazon EC2 [18]. In 2009, all of sudden this service went down. As a result, whole production came down. Problem continued for several hours (19 hours approx.), before the services were restored. Once the Amazon pin pointed the problem, and then only it could be put on [18].

5 Conclusion

Security in cloud computing is a critical issue considering the privacy and regulatory acts. A number of organizations and working group are putting their efforts to strengthen the security in cloud computing. Working groups are releasing their drafts and report on critical security threats and recommending various methods to counter them. Although various study reveals that hosted model is more secure relative to the on-premises cloud model. Yet, many attacks are targeting the hosted model to exploit the vulnerabilities. DDoS and Phishing are the major method employed to attack the cloud. Finally, in the light of phishing and DDoS attack that took place in many of the cloud revealed, it can be concluded that they are causing huge financial losses, damage to privacy of data. Although a number of solutions are existing that are countering various attacks, still there is further need to strengthen the security in hosted as well as on premises cloud, in order to restore the confidence of users.

References

[1] AlertLogic, “Targeted attacks and opportunistic hacks, state of cloud security report spring 2013”, available at https://www.alertlogic.com/alert-logic-releases-2013-state-of-cloud-security-report/.

[2] Arbor, “Arbor Special Report: Worldwide Infrastructure Security Report”, Volume IX, 2014, available at http://pages.arbornetworks.com/rs/arbor/images/WISR2014.pdf.

[3] J. Archer, A. Boehme, D. Cullinane, P. Kurtz, N.J. Reavis. “Top threats to cloud computing”, version 1.0. Cloud security alliance retrieved 7 May 2011, accessed from http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[4] B. Boss, P. Malladi, D. Quan, L. Legregni, and H. Hall “Cloud computing”, 2009. http://www.ibm.com/developerswork/websphere/zones/hipods/library.html.

[5] E. Chickowski, “Sony Still Digging Its Way Out of Breach Investigation”, Fallout ,02 Apr 2013, available at http://www.darkreading.com/attacks-breaches/sony-still-digging-its-way-out-of-breach/229402823.

[6] M. Cobb, “How cyber-criminal attack the cloud”, information week (dark reading), (2013), available at http://www.darkreading.com/attacks-breaches/how-cybercriminals-attack-the-cloud/240153610.

[7] CSA (2013), “The Notorious Nine Cloud Computing Top Threats in 2013”, Available at https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_ Nine_Cloud_Computing_Top_Threats_in_2013.pdf.

[8] CSA, “Top Threats to Cloud Computing”, 2010, V1.0.

[9] Ericka Chickowski,Sony Still Digging Its Way Out of Breach Investigation, Fallout ,02 Apr 2013, available at http://www.darkreading.com/attacks-breaches/sony-still-digging-its-way-out-of-breach/229402823.

[10] A. Goscinski, M. Brock, “Toward dynamic and attribute based publication, discovery and selection for cloud computing”, *Future Generation Computer Systems*, vol. 26, pp. 947-970, 2010.

[11] C. Green, “Dropbox hit by Zeus phishing attack”, Oct 2013, available at http://www.information-age.com/technology/security/123457411/-dropbox-hit-by-zeus-phishing-attack.

[12] A. Hall, “Recent phishing attack targets select Microsoft employees”(accessed on 24 Jan 2014) available at https://blogs.technet.com/b/trustworthycomputing/archive/2014/ 01/24/post.aspx (accessed on 01 Feb 2014).

[13] B. Hayes, “Cloud computing”, *Communications of the ACM*, vol. 51, no. 7, 2008.

[14] A. Hutchings, R.G. Smith, and L. James “Cloud computing for small business: Criminal and security threats and prevention measures”, Trends & issues in crime and criminal justice, no. 456, May 2013.

[15] IBM, “Security service cyber security intelligence index”, IBM Global technology services security services, 2011

[16] IMPERVA, “Hacker intelligence initiative”, Monthly Trend Report. Report no. 18, Dec 2013.

[17] D. Marcus, D. and R. Sherstobitoff, “Dissecting operation high roller”, Mcfee, white paper, 2012, available at http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf.

[18] P. Mell, and T. Grance, "The NIST definition of cloud computing", Special Publication 800-145, National Institute of Standards and Technology, 2011, available at http://csrc.nist.gov/ publications/ PubsSPs.html#800-145.

[19] C. Metz, “DDoS attack rains down on Amaon cloud”, Oct 2009, available on http://www.theregister.co.uk/2009/10/05/amazon_bitbucket_outage/(accessed on 1 Feb 2014).

[20] NIST, 2011, NIST cloud computing program retrieved 21 May 2011, fromhttp://www.nist.gov/itl/cloud/.

[21] B. Prince, "Spamhaus DDoS attack renews talk of DNS server security", Apr 2013, available at http://www.darkreading.com/attacks-breaches/spamhaus-ddos-spotlights-dns-server-secu/240152167.

[22] S.H. Shin, and K. Kobara, “Towards secure cloud storage”, *Demo for CloudCom2010*, Dec. 2010.

[23] S. Srinivasamurthy, and D. Q. Liu, "Survey on cloud computing security", *in Proceeding of Conference on Cloud Computing (CloudCom.'10)*, 2010.

[24] Md. Tanzim Khorshed, A.B.M. Shawkat Ali & Saleh A. Wasimi, “A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing”, *Future Generation Computer Systems*, vol. 28, no. 6, pp. 833–851, 2012.

[25] Verizon,"The truth about DDOS Attacks", 2013, available at http://www.verizonenterprise. com/ products/security/managed/.

[26] R. Westervelt, “Phishing attack, stolen credentials sparked South Carolina breach”, available at http://searchsecurity.techtarget.com/news/2240172466/Phishing-attack-stolen-credentials-sparked-South-Carolina-breach?asrc=EM_NLN_19698566 &track=NL-102&ad=883490.

[27] D. Windser, “Databases in the cloud- a new target for cyber criminals”, CloudPro, 2013, available at http://www.cloudpro.co.uk/cloud-essentials/cloud-security/3639/databases-in-the-cloud-a-new-target-for-cyber-criminals.

[28] G. Wrenn, CISSP, ISSEP, Unisys Secure Cloud Addressing the Top Threats of Cloud Computing, (online) (2010), White Paper, http://www.unisys.com/unisys/unisys/inc/pdf/whitepapers/38507380-000.pdf (accessed May 26, 2011).

[29] L. Yan, C. Rong, G. Zhao, “Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography”, *in Proceeding of 1st International Conference on Cloud Computing (CloudCom 2009),* pp. 167-177, Beijing, China, Dec. 1-4, 2009.

Jitendra Singh has pursued his masters in computer science that is followed by PhD in computer science, in the area of cloud computing. He has qualified the prestigious UGC-NET examination conducted by the UGC of India. He has more than 11 years of teaching experience. During his academic career, he has taught to the students of Bachelor and Master Courses. He is also involved with the Stratford University, USA, India Campus, as a part time faculty from more than 2 and half years. He has contributed more than dozen of research papers in the area of cloud computing. Many of them are published in reputed journals. In addition, he is also author of two books titling ‘Cloud computing for beginner to researcher’ and ‘Data structure simplified: Implementation using C++”. His research areas of interest are cloud computing, Networking, Security, etc.

Establishing Safe Cloud: Ensuring Data Security and Performance Evaluation

Masoumeh Zareapoor, Pourya Shamsolmoali, and M. Afshar Alam
(Corresponding author: Pourya Shamsolmoali)

Department of Computer Science, Jamia Hamdard University[1]
New Delhi, India
(Email: pshams@jamiahamdard.ac.in)

(Received May. 16, 2014; revised and accepted Aug. 9, 2014)

Abstract

Cloud computing are threatened by unresolved security issues that harmful for both the Cloud providers and Cloud users. The aim of this paper is divided into three parts; firstly an exclusive review on grid and cloud computing, the main focus concerned on security. Secondly recognize top threats, their accessible solutions and discover unique security requirements for cloud computing. Thirdly present a solution that eradicates possible threats. In particular, we proposed a novel data security model that can efficiently protect the data whether in the cloud database or at the time of transition. We commence with establish of Authentication server and Data server to provide user authentication, user verification and data support. The model followed by using SSL (Secure Socket Layer) protocol to encrypt and protect the data in time of transition. SDR (Secure Delivery Report) is used to ensure the reliability, authenticity and integrity of communication and data.

Keywords: Authentication; Cloud computing; Data protection; Encryption; Security

1 Introduction

Today Grid computing fundamentally plan to enable access to high performance distributed resources in a regular and simple way. In grids, Users can create state full services to increase complex and computation-intensive tasks. This is achieved by means of a middleware standard: every host has a grid boundary, and developers accept middleware-dependent APIS for building up their applications. Cloud Computing brought us an innovative feature of Internet and data storage. The cloud offers massive benefits to businesses, since do not require spending huge amount on expensive software or hardware that they might never call for. A definition by Valentina et al.; and Foster et al. declares that cloud is a large-scale distributed computing that is taken by economics of scale, in which a group of virtualized, managed computing power, platforms, storage and services are delivered [1, 2]. NIST provided a definition, which depicts cloud computing as a model for permitting convenient, for accessing network to a shared lake of computing resources (e.g. storage, servers, applications and services) in comparing with traditional networking method cloud computing can be quickly provisioned and released with minimal management endeavor or interaction of service provider. Providers of service must make certain that they get all the security facets right, and if things go wrong, they are the ones who will responsible. Lots of advantages like lower costs, pay-for-use, fast deployment, scalability, ubiquitous network access, low-cost disaster, data recovery, data storage solution and greater resiliency offered by cloud.

Cloud computing moves the application software and databases to the vast data centers, where the management of the services and data are not reliable. These unique aspects on the other hand create many new security challenges [3]. These challenges include but not limited to access vulnerabilities, web application vulnerabilities, virtualization vulnerabilities, problems related to data verification, problems related to credential management and identity, integrity and issues related to authentication of the respondent devices. As cloud computing is getting increased reputation, concerns are being expressed about the security issues introduced through the approval of this new model. The efficiencies of traditional defense mechanisms are being reconsidered, as the attributes of this new deployment model [4]. In this paper we concentrated on cloud computing with the main focus on security. The data security model is considered and unique security requirements are documented.

The reminder of this paper is structured as follows: section 2 covers the review of grid and cloud. Section 3 describes the cloud computing security and list of top security threats. Section 4 describes data security in cloud .Section 5 covers the proposed model. Section 6 describes the security proof of proposed model. Section 7 covers the performance evaluation. As a final point, section 8 documents some conclusions.

2 Review of Grid and Cloud Computing

Thought of Grid computing for first time appeared in 1990s, as high performance computers were internally connected. A simply explanation for Grid computing is “a hardware and software component that presents dependable, reliable and low cost access to end of computational capabilities”. Gao et al. [5] have done a systematic review of communication/networking technologies in smart grid that mainly focused on communication/networking architecture, quality of service (QOS) and optimizing utilization of assets. Cloud computing can be resulted from advancement and convergence of Grid computing. Foster et al. [2] declare that “cloud computing is not absolutely new thought, it has connection to the Grid computing and other significant technologies such as distributed systems cluster computing and utility computing”. One of recent Grid workgroup, EELA-2 e-Infrastructure is consisted of grid service and a grid opportunistic that associate computing resources from scientific institutions in Latin America and Europe [6]. Cloud computing name, was motivated by the cloud symbol that is frequently used to represent the internet in flow charts and graphs. A distinct migration to the clouds over recent years has been taking place by end users, step by step number of private data, such as snaps and song files are growing on remote servers and easy to get via a network. Cloud computing is made powerful by virtualization technology: This technology that actually started since 1967, but it was only existing for mainframe systems. By using this technology, we can create one or more virtual machines by running an application on host computers called as a hypervisor, and can test any software from virtual machine operating system [4]. At a datacenter or hardware level a number of physical devices such as, network devices, hard drivers and processors are located, which are responsible for handling processing and storage needs. On top of this level, group of virtualization layer, the software layer and the management layer have responsibility to manage servers. Zissis and Lekkas [4] Note that virtualization is a significant element in implementation of cloud and provide the necessary cloud features of resource pooling and location independence. In simple view Cloud and Grid are using same technologies, the only technology uses in cloud computing and makes it new and different from Grid computing is virtualization. Unlike grid computing, Cloud computing leverage virtualization to take full advantage of computing power. Virtualization, answered some of the problems faced in grid computing by separating the physical from logical [7]. Harris [8] notes that grid computing realizes high operation through the allocation of several servers onto a single task or job, the virtualization of servers in cloud gets high utilization by allocating one server to compute several tasks at the same time. Mauch et al. [9] have done an overview on the current state of high performance cloud computing technology and also describe the underlying management methods and virtualization techniques. Zhao et al. [10] introduced an integrated framework and the graphical grid user interface that can be used by cloud users to access the underlying services. Most of authors and researchers have same opinion and statement that cloud computing has developed from grid computing and grid is the base of cloud computing. Cloud inherits all the existing security issues and the issues that has been created due to its exclusive framework and features from existing technologies.

Location independence is a sense of cloud computing, the user normally has no control or knowledge over the real location of the resources. But maybe at a higher level of abstraction like datacenter be able to specify location. Implementation of cloud contains advanced security technology, generally available due to the centralization of data and standard architecture. Khorshed et al. [11] have drawn a Figure which makes it simple to understand cloud system and the main features. Other authors [12, 13, 14, 15] who also tried to note and arrange different aspects of cloud computing. By review of all these research we have constructed a new diagram to show the aspects of cloud, as shown in Figure 1.

In Figure 1 we have classified a system of cloud into eight major aspects. They are features, layers, roles, service delivery models, deployment models, comparison, locality and security. All of these aspects have minimum three sub aspects. We connected all sub aspects to the related major aspects.

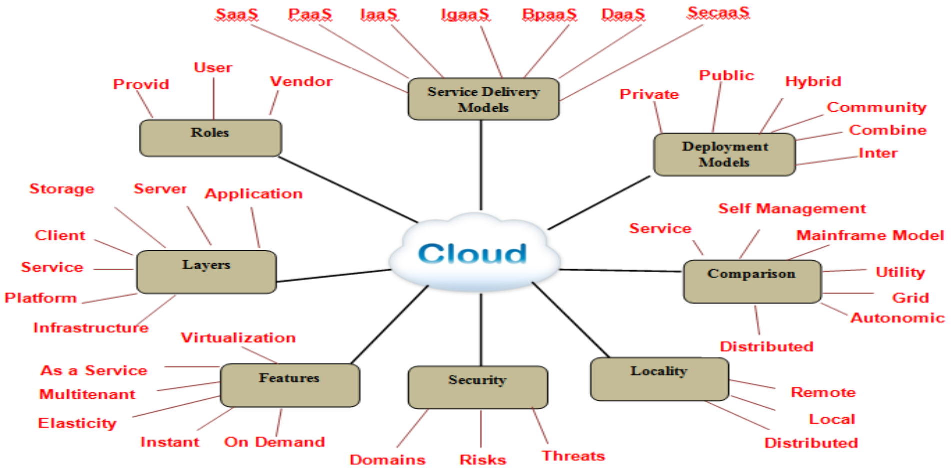


Figure 1: Different aspects of cloud computing

3 Cloud Computing Securities

Security in cloud computing is controlling the access of unauthorized users to the system state. The main aspects of security are confidentiality, availability and integrity [16]. Confidentiality means, assuring the users that there information will not disclose without their authority. Availability is a process of ensuring, the information are available to the end users whenever and wherever they need. Integrity is avoidance of the unauthorized modification or information deletion.

3.1 Cloud Computing Security Review

At this time, there are several research works happening in the area of cloud security. Various research groups and organizations are trying to develop security solutions and standards for cloud. The cloud security Alliance (CSA) is solution provider and non-profit organization, offer common level of understanding, consciousness and guidelines for cloud related security threats [17]. A society in United States government called as, The National Institute of Standard and Technology (NIST); their long term aim is to offer precise guidance to the industry, provider and government and their plan to identify security threats in cloud standards [18]. Subashini and Kavitha [19] have done a survey on different service delivery models in cloud computing and they discuss all security issues of service delivery models. Vazquez *et al.* [20] made a note on use of clouds for grid resource provisioning; offer architecture for building multipart grid infrastructures able to sustain the demand required by any given service. Srinivasamaurthy and Liu [21] have done a survey on different security threats and advantage of secure Cloud design.

The authors present novel method to reduce these threats. Habib et al. [22] have done a survey on trust as a facilitator that mainly focused on cloud computing from the perspective of cloud consumer. Srivastava et al. [23] have done analyze on the security landscape and propose architecture based on proactive model, the authors consider on two cloud deployment models, privet and public and suitability for adoption in an enterprise environment, and how these models behave on different threats. Khorshed et al. [11] draw a diagram that organized cloud computing security into three sections: security dimensions, security categories and security in service delivery models. Cloud Security Alliance (CSA) published version 3.0 of their document “Security Guidance for Critical Area of Focus in Cloud Computing” in November 2011, they recognized fourteen areas of concerns in three main section. “Section 1: cloud architecture, Domain 1: Cloud computing architectural framework; Section 2: Governing in the cloud, Domain 2: Governance and enterprise risk management, Domain 3: legal issues: Contracts and electronic discovery, Domain 4: Compliance and audit management, Domain 5: Information management and data security, Domain 6: Interoperability and portability; Section 3: Operating in the cloud, Domain 7: Traditional security, Business continuity and Disaster recovery, Domain 8: Data center operations, Domain 9: Incident response, Domain 10: Application security, Domain 11: Encryption and key management, Domain 12: Identity, Entitlement and Access management, Domain 13: Virtualization, Domain 14: Security as a service; ” [17].

Blasidell [24] have done a research on top threats to cloud computing, he recognized four threats for cloud “Threat no 1: Security threats, Threat no 2: Outages, Threat no 3: Malicious insiders, Threat no 4: Lack of information; ” CSA also published another research work on the top threats to cloud computing in March 2010. The point of the research was to support cloud providers and consumers in identifying the main vulnerable points and major risks of cloud, and also, how cloud provider can infrastructure from these risks. It is our contention that CSA on cloud computing security could be considered as pioneering work to direct aspiring future researchers to protect them in this area. We have found CSA's research on top threats [25] is latest among the distinguished research works in cloud computing security area, and not lots of reviews are presented on it, we have decided to expand on the seven top threats in next section.

3.2 Cloud Computing Top Threats Overview

Security in computer network is a difficult task. Especially in cloud computing that it has nature of shared on-demand. Choice of a proper security procedure needs accurate judgment of threat environment [25]. The top threats of cloud computing according to the CSA are introduced as follows.

3.2.1 Abuse and Nefarious Use of Cloud Computing

CSA pointed the cloud service provider (CSP) in Infrastructure-as-a-service (IaaS) do not sustain sufficient control. Spamming, phishing, hacking and other types of people engaged in criminal activities can take benefit of the chances such as free limited trials periods. PaaS providers have usually suffered most from this kind of attacks; on the other hand, current proof shows that hackers have begun to object IaaS provider as well. So, if a malicious or attack happen, CSP not able to directly knows, and have to rely on other mechanisms such as warning and abuse report. Future areas of concern include password and key cracking, hosting malicious data, DDOS, launching dynamic attack points and botnet command and control. CSA proposed strict registration and validation procedures, coordination and enhanced monitoring for credit card frauds, comprehensive introspection of user network traffic and public blacklist monitoring [25].

3.2.2 Insecure Application and APIs

As cloud service providers provision some type of software interfaces or APIS to a user to manage and cooperate with cloud services. A comparatively weak APIS or too much gateway interfaces may expose different kinds of security problems. The security and access to universal cloud service models is dependent upon the security of these basic APIS. CSA suggested solutions to minimize the problems and to analyze the security model of cloud provider interface, to make certain strong authentication and access control with encrypted transition and understanding the reliance chain associated with the API [25].

Sirisha and Kumari [26] propose a model to ensure a two stage security at the API level. The first step to ensure that, only registered users can have access to cloud services and the second step, getting power of Role Based Access Control. Andrei and Jain [27] commended the use of API in cloud computing for it centralized model. They beloved cloud helps software developers in generating several evaluation environments for their applications. Monitoring of software can be happen by monitoring API calls for server requests. If there be a centralized architecture for data storing, all efforts can be focused in one route resulting to improve monitoring. Khorshed et al. [11] note that there are some benefits of monitoring API in cloud computing based centralized system, but web application based API generally share more vulnerabilities.

3.2.3 Malicious Insiders

Malicious insider threat is familiar to all organizations this threat is intensified for users of cloud services by the convergence of IT services and users under a single management domain. It is common for a provider to conceal its own company policy on recruiting employees and provide different level of access to them, but with higher level of access an employee can increase access to private data and services. CSA recommend strict supply chain management and perform a comprehensive supplier assessment. Specify human resource requirements as part of official contracts or we can call it Service Level Agreement. Require transparency into overall information security and management practices, as well as agreement reporting. And determine security breach notification processes [25].

Srivastava et al. [23] note that "the best prevention way against insider threat is a strong and effective organization security policy". Khorshed et al. [11] discussed that, there are lots of proposed solutions for insider threats, but these solutions come into effect after a serious security violate arises. In the foreseeable future, it is a cloud provider tendency to hide from view its company policy regarding hiring of employees and put in place insufficient measures to monitor them because of financial reasons. Spring [28] recommended ten most excellent practices for cloud providers to control malicious insiders. These are: least privilege, separation of privileges, alarm systems, access control systems, administrator logging, two factor authentication, codes of conduct, confidentiality agreements, visitor access and background checks.

3.2.4 Shared Technology Vulnerabilities

Cloud computing has a nature of shared on-demand and it asks for virtualization technology, and virtualization applies hypervisors to generate virtual machines and operating systems. But a single misconfiguration or flow in a hypervisor allow malicious to achieve inappropriate access and control to the platform that hits the rest of users as well. A depth action of defense is recommended in IaaS model, and supposed to include monitoring, storage and network security. CSA proposes implement security best practices for installation, configuration and monitoring of environment for unauthorized activity and changes. Promote heavy authentication and access control for administrative. Service Level Agreement (SLA) for patching and vulnerability remediation and conduct vulnerability scanning and configuration audits [25]. Srivastava et al. [6] pointed that hypervisor is a fundamental product for IaaS vendors and when infrastructure is sharing by many different clients, the security build upon the robustness of the underlying hypervisor. Grobauer et al. [29] presented new model for virtualization technology and VMs image handling. As a regular method, cloud service providers build a template image of OS and copy it to several machines. This manner is vulnerable due to an attacker can get rent a VM and can get access to the secret information of users and administrative configuration as well. Addition significant issue they raised is that even an image can be achieved from an untrustworthy source, which my offer back-door access to an attacker. Khorshed et al. [11] analyzed that there are an expectation for virtualization technology in the near future and virtual servers to be established from computational resources. Lombardi and Pietro [30] proposed an architecture called as "Advanced Cloud Protection System". It can be deployed on multiple cloud solutions and can efficiently monitor the reliability of guest virtual machines and infrastructure components. Li et al. [31] analyzed the security challenges faced by green cloud computing, and proposed a virtualization security assurance architecture, which is designed to address multiple key security problems with the cloud computing.

3.2.5 Data Loss (Leakage)

Cloud provider must give guaranty to cloud users that their cost saving methods never compromise users valuable data as there are numerous ways to compromise data. The methods particularly increase in environment of cloud computing due to the number of interactions between risks and challenges. An example can note deletion or alternation of records without backup of the main content and other example can be mention here is, not able to recover large context after disaster. Also loss of an encoding key can be very harmful. Some of these may be unique to cloud as well as very difficult because of cloud architecture [25]. CSA suggested solutions include implementing of strong API access control, Encryption and integrity protection of data in transit, Analyzes of data protection at design as well as runtime, implementing strong key generation, storage and management, and destruction practices, contractually demand providers wipe persistent media before it is releasing to the pool. Contractually specifies provider backup and retention strategies [25]. Srivastava et al. [23] mentioned data loss or leakage is one of painful threat in the cloud technology. Because of the structure of cloud, an organization data may locate in servers in some other nation. This is a major concern for some organizations. One more issue is that how long the data may be retained by the service provider. The data may remain on the servers even after it has been removed by the client. Dahbur et al. [32] note that if employees and users of cloud are not educated enough on processes and procedures, they cloud make intentional or unintentional mistake that can be reason of data loss or leakage on a business. Data protection has a high priority in network security, but in cloud computing it reaches a much higher level of challenge because of the number of interactions between risks and challenges. While unchecked procedures and inadequate data retention practices are very common, they might be dangerous in cloud computing because of policy issues and complex infrastructure [11].

3.2.6 Account or Service Hijacking

These kinds of attack are not new and generally performed by stolen credentials. There are lots of attack method for stealing someone credentials such as Phishing, Denial of Services (DOS), fraud, Software vulnerabilities and account hijacking. In a cloud area, if an attacker can gain access to your credentials, he or she can eavesdrop on your activities, transactions and control data. Proposed solutions by CSA include prohibit on the sharing of account credentials between services and users. Leverage strong two-factor authentication techniques wherever possible, employing proactive monitoring system to detect unauthorized activity. Understanding cloud provider security policies and service level agreements (SLA) [25]. Revar and Bhavsar [33] designed and implemented an optimized infrastructure for secure authorization in cloud computing environment; this architecture only consists of the authentication mechanism on the Single Sign-On (SSO) servers. Srinivasamurthy and Liu [34] pointed four types of attack that match to these kinds of threat. There are: Phishing, man in the middle attacks, spam campaigns and DOS attacks. Chandwick and Fatema [35] developed a policy authorization that a cloud provider can deliver an infrastructure service to its users. It will secure the user's data privacy by allowing the users to set their own privacy policies and enforcing them, so that no unauthorized access is allowed to their data. This structure guarantees that the users' privacy policies are stuck to their data, and access will constantly be controlled by the policies even if the data is moved between clouds.

3.2.7 Unknown Risk Profile

One of the main theory of cloud computing is the reduction of hardware and software needs and maintenance to allow cloud users to focus more on their actual business. This has financial and operational saving. Though, shifting into the cloud environment may not ensure the effectiveness of the security procedures that the company used to control by itself, and can bring about unknown risks. Suggested solutions by CSA include disclosure of applicable logs and data, partial or full disclosure of cloud infrastructure, and monitoring and altering on all important information [25].

Table 1: Top security threats of cloud computing

Threats	**Vulnerable Service Models**	**Security Requirements**
Abuse and nefarious use of cloud computing	• PaaS • IaaS	• Hardware security • Network protection
Insecure application and APIs	• SaaS • PaaS • IaaS	• Network resource protection • Communication security
Malicious insiders	• SaaS • PaaS • IaaS	• Virtual cloud protection • Access control
Shared technology vulnerabilities	• IaaS	• Application security
Data loss /leakage	• SaaS • PaaS • IaaS	• Cloud management control security • Secure images • Data security
Account or service hijacking	• SaaS • PaaS • IaaS	• Software security • Service availability
Unknown risk profile	• SaaS • PaaS • IaaS	• Access control • Privacy in multitenant environment

CSA raised in this text their attention about users' questions that are not cleared by cloud providers. In another statement they commented "unless cloud providers can readily disclose their security controls and the point to which they are implemented to the user and the user knows which controls are needed to maintain the security of their information, there is tremendous potential for misguided decision and detrimental outcomes" [25]. We accordingly get that an unknown risk profile is something creation of the cloud providers' unwilling in providing points about security practices, audit report, security logs and etc. [17, 25]. Without these points users can not grasp entire level of security procedure and maybe exposed to unknown risks. Most of the solutions are difficult due to the aversion of cloud providers to be transparent in this issue.

In table 1 we have done a review on top security threats of cloud computing and we have noted the vulnerable service models that each threat can do effect. We have listed the minimum security requirements that cloud providers have to maintain in their infrastructures and systems.

4 Data Security in Cloud

The main weakness that traditionally correlated with cloud computing is the lack of arrangement for data security and the perception of moving to the cloud, make critical data to be uncovered at the time of attack [36]. It is depend to the form of cloud computing, policies and management. Mackay et al. [37] summarized three specific data storage security issues in the cloud that any service provider suppose to attend, the first mechanism to apply is encryption whereby all data stored in the cloud is encrypted. The second issue is shared resources. The last issue to consider is the integrity of the data that migrate to cloud storage. Rong et al. [38] pointed that the owner of data should have full control over authorization of data sharing. With authorization given by the data owner, selected user can have access to data stored on the cloud [39]. This action should not provide the service provider any right to access the user's data.

5 Proposed Model

In this section, we present a framework that has been structured to offer absolute solutions to preserve the integrity, confidentiality and authenticity of data and communications. We applied multiple techniques and mechanisms such as verification of the digital signature and double authentication to protect the critical data from unauthorized users.

The system consists of three main parties:

Cloud Provider: who manages, provides cloud storage services and has high computation power.

Data Owner: organizations or an individual customer who has vast data files to be stored in the cloud storage.

User: who will register with data owner and uses or shares a data stored on cloud storage. The user has limitation right to use data files.

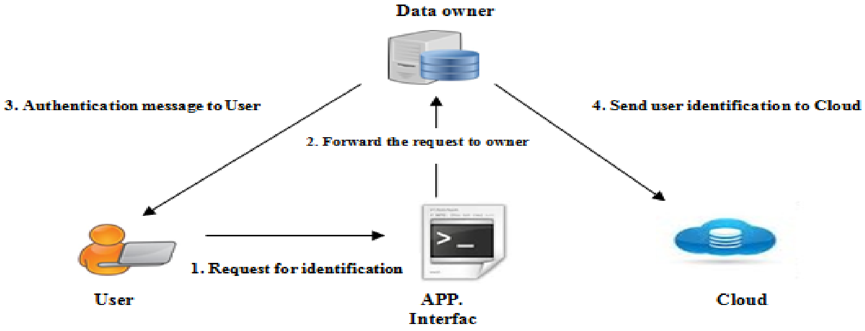

Data owner
3. Authentication message to User
4. Send user identification to Cloud
2. Forward the request to owner
1. Request for identification
User
APP.
Interfac
Cloud

Figure 2: User registration process

In proposed model as shown in Figure 2, when a user wants to access the data stored in the cloud, first of all needs to register with the data owner by getting a valid username and password through the application interface. Next the Data Owner sends authentication message (User name and Password) to the user. At the end the owner forwards the registered ID to cloud to store it within the user directory of the authentication server.

The abstract flaw in Figure 3 illustrated the interaction between the four parties and it consists of the following steps.

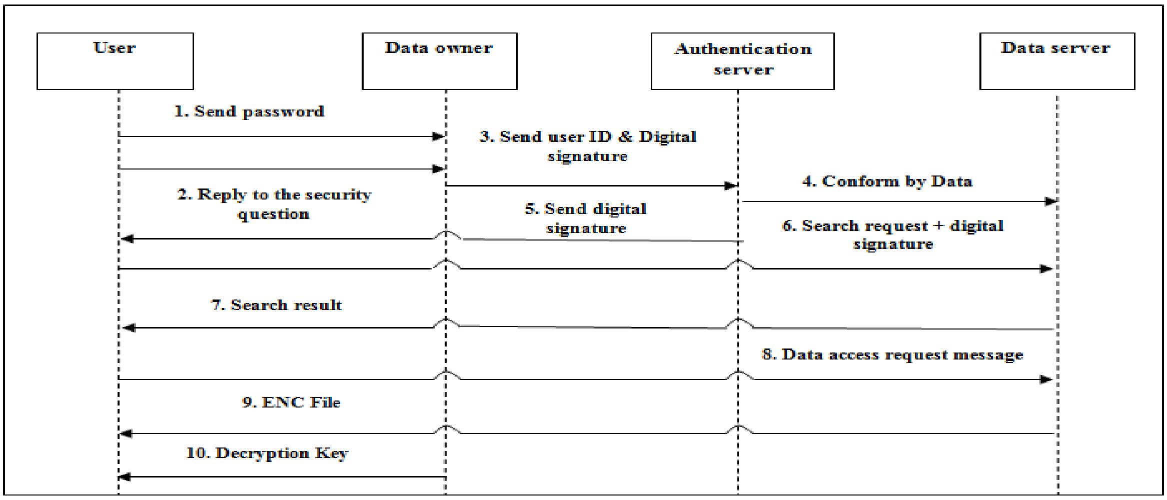

User
Data owner
Authentication server
Data server
1. Send password
3. Send user ID & Digital signature
4. Conform by Data
2. Reply to the security question
5. Send digital signature
6. Search request + digital signature
7. Search result
8. Data access request message
9. ENC File
10. Decryption Key

Figure 3: Object oriented design of proposed model

1) The user sends the user ID and password to the data owner. First level of authentication.

2) The user replies the security question provided by data owner. Second level of authentication.

3) The data owner redirect the user ID and digital signature to Authentication server, therefore cloud will be sure that the owner let user access of data.

4) The Authentication server validates the user approval and authorization grant. It also validates that the user is a trusted entity by data server and issues access permission.

5) The Authentication server forwards the digital signature to the user. The user use it as an authentication token.

6) The user afterwards sends the search request and asks for protected resources by presenting digital signature to Data server.

7) The Data server responds to the search request and delivers the search result to the user.

8) The user generates a request to the data server for retrieving the encrypted data.

9) Afterwards the Data server sends back the requested data in encrypted format.

10) Then the Data owner dispatches the decryption key to the user.

6 Security Proof

6.1 Confidentiality of Data

Secure travelling of data on the network is a tough and highly complex issue, while the data threat is continuously raising and improving. In the cloud environment it does not only require traffic protection in addition secure way of communication also essential [4]. To prevent the loss of data in transition, SSL (Secure Socket Layer) protocol in our model is used. SSL generates end-to-end encryption by interacting between applications and the TCP/IP protocols to present authentication and an encrypted communications between Data owner, Server and User. SSL protocol is available into every web browser, so do not require any special software to install in the user system. To create secure communication between data server and User first the data server sends the identification information to the user just after the connection creates then sends the user a copy of its SSL certificate. The user verifies the certificate and replies to the data server. The data sever sends back a token to build SSL session.

6.2 Limitation of Service Provider in Data Access

When the data reside in a cloud database, all the management and responsibility are by service provider. Assume that, the data in a cloud database are secure from any external party, as the service provider uses strict security roles to protect his environment. The service provider can oppose the data owner. As the data in a cloud is not in the direct control of the owner, any harm can be possible by cloud service provider. So the service provider cannot be fully trusted. For this problem the best solution applied in proposed model is encryption of data before storing in the cloud. Integrity, confidentiality and privacy of data can be protected through encryption [4]. SSL protocol as we explained in previous section encrypts the data and builds private and secure communication over the public internet.

6.3 Loss/Leakage of User ID

Authentication is required in cloud computing to restrict the boundary of access for unauthorized user [40]. Therefore, if any user looses or accidentally discloses his\her user ID and password to any illegal user, it can make problems for data privacy. To protect the data, we inserted an additional parameter, which is must to pass in order to access the data in the cloud database. In this step the system asks a security question whose answer is known only to the authorized user. So this security parameter can control the access of the unauthorized person to the data.

6.4 Secure Delivery Report (SDR)

The data in the cloud is always vulnerable and under the threat of being interfered by any attack. As all the precautionary methods such as double authentication, data encryption and using SSL protocol in the proposed model to not allow anyone interfere to the data at transition time. The model has one more parameter called as Secure Delivery Report (SDR). Firstly SDR generates by the data owner before send the data to cloud, the owner keep the SDR in his memory. On another side, when the user receives the data can generate the SDR of received data and sends it to the data owner, the data owner can compare the new SDR with the original one that he has. If both the SDR are same, the user is assured the data has not been interfered. In case the owner gets that the SDRs are not same, a message is generated to cloud to resend the data file to the same user. As shown in Figure 4.

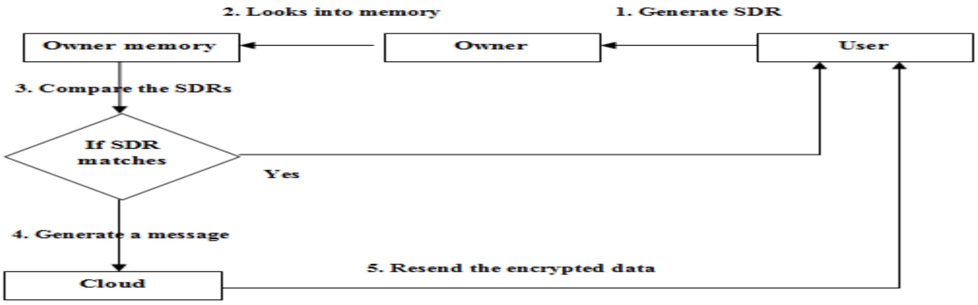


Figure 4: Secure delivery report

7 Performance Evaluation

An effective data security model should be able to overcome all the existing issues of cloud computing to prevent the owner's data from all the risks associated, in Table 2 we have done a comparison between other data security models and the proposed model.

The proposed model is evaluated with respect to implementation. This model is tested on CloudSim Simulator. That it is a framework for design and simulation of Cloud infrastructures and services [43, 44]. Figure 5 represents the status of security after implementation of security parameters that is SDR, Identification & Authentication and Encryption. Encryption provides additional security than Identification & Authentication and it provide more security than SDR.

Table 2: Comparison of data security models

	Wang et al.[3]	Prasad et al.[41]	S.K. Sood.[39]	Proposed Model
Authorization	Yes	Yes	Yes	Yes
Confidentiality	Yes	Yes	Yes	Yes
Integrity	Yes	Yes	Yes	Yes
Encryption	Yes	Yes	Yes	Yes
Identification and authentication	Yes	Yes	Yes	Yes
Data security even after loss of user ID	No	No	Yes	Yes
User verification	No	No	No	Yes
Secure Delivery Checking	No	No	No	Yes

However by taken the combination of all three security parameters as mentioned in Figure 5 the security of data has the best efficiency. It shows the security evaluation of our proposed model.

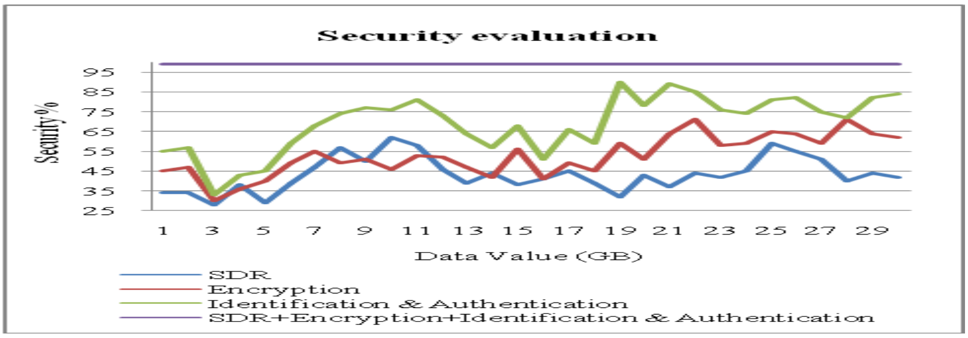
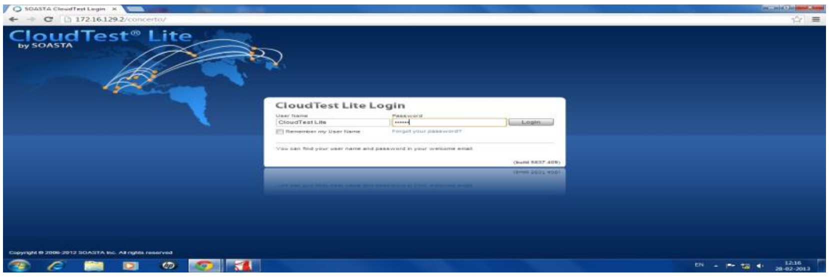


Figure 5: Security evaluation

To create a virtual cloud environment, we have used a HP Proliant DL 580 G7 Server, with following features: dual 1.864 GHZ processors, 16 GB RAM, 5×300 GB SCSI Hard Drives build on 474610. We also selected VMWare ESXi 5.0.0 Hypervisor as virtual machine manager (VMM) and windows 7 as guest operating system. For monitoring, load and performance Testing we used Cloud Test Lite by SOASTA [42].



SOASTA CloudTest Login

172.16.129.2/concerto/

CloudTest® Lite by SOASTA

CloudTest Lite Login

User Name: CloudTest Lite

Password: ••••••

Login

□ Remember my User Name

Forgot your password?

You can find your user name and password in your welcome email.

(build 5837.409)

Copyright © 2006-2012 SOASTA Inc. All rights reserved

EN 12:16 28-02-2013

Figure 6: SOASTA login page

Previously we show the security performance of our proposed model. After implementation of all security parameters Performance of Database connection pool usage, CPU utilization and Memory usage in five minutes illustrated in Figures 7, 8 and 9.

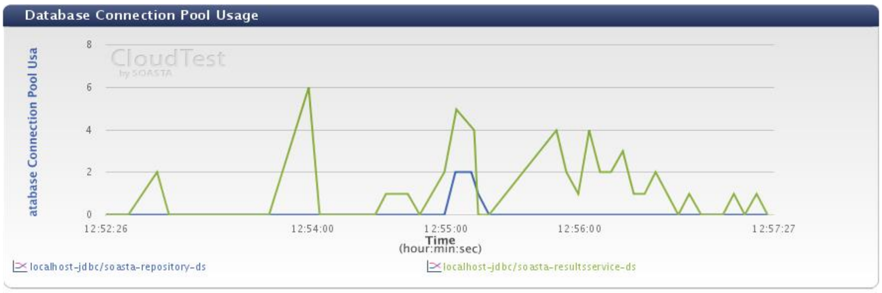


Figure 7: Database connection pool usage

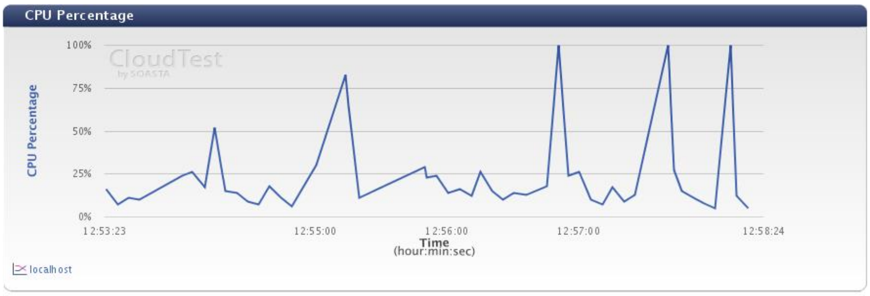


Figure 8: CPU utilization

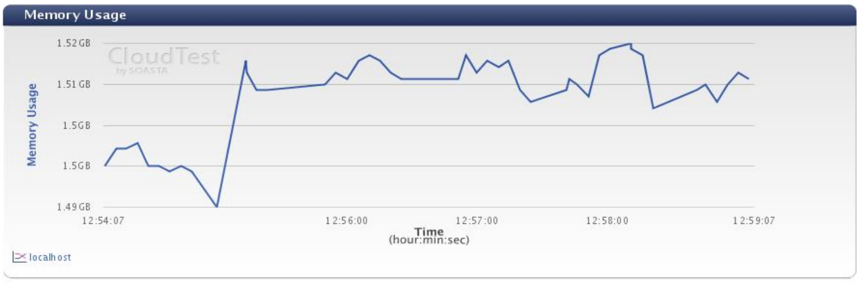


Figure 9: Memory usage

The Figurers illustrate that. The proposed model has a very good performance as compare to different models.

8 Conclusion

This paper proposed a novel model; it contains the security and performance issues. In first step, we used the technique of double authentication of user, we synchronized an authentication model between the User, Data Owner, Authorization Server and Data Server also verification of digital signature of the data owner. In the second step, we used SSL protocol for encryption and prevent the loss of data. In the third step, we used Secure Delivery Report (SDR) to check the integrity of data. We believe that our proposed model ensure data traversing in cloud computing environment.

Acknowledgements

We would like to thank Dr. Antonio Cuomo for his helpful comments that helped to improve the quality of the paper.

References

[1] V. Casola, A. Cuomo, M. Rak, U. Villano, "The CloudGrid Approach: Security analysis and performance evaluation", *Future Generation Computer Systems*, vol. 29, no. 1, pp. 387-401, Jan. 2013.

[2] I. Foster, Y. Zhao, I. Raicu, S. Lu, "Cloud computing and grid computing 360- degree compared", *in Grid Computing Environments Workshop*, pp. 1–10, 2008.

[3] C. Wang, Q. Wang, K. Ren, "Ensuring data storage security in cloud computing, Cryptology eprint Archive" Report, 2009. (http://eprint.iacr.org/)

[4] D. Zissis, D. Lekkas, "Addressing cloud computing security issues", *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583-592, 2012.

[5] J. Gao, Y. Xiao, J. Liu, W. Liang, C.L.P. Chen, "A survey of communication/networking in smart grids," *Future Generation Computer Systems*, vol. 28, no. 2, pp. 391-404, 2012.

[6] F. Brasileiro, M. Gaudencio, R. Silva, A. Duarte, D. Carvalho, D. Scardaci, et al., "Using a simple prioritisation mechanism to effectively interoperate service and opportunistic grids in the EELA-2 e-Infrastructure," *Journal of Grid Computing*, vol. 9, no. 2, pp. 241–257, 2011.

[7] Merrill Lynch, The cloud wars: Merrill Lynch, 2008.

[8] D. Harris, Why 'grid' doesn't sell, 2008.

[9] V. Mauch, M. Kunze, M. Hillenbrand, "High performance cloud computing," *Future Generation Computer Systems*, vol. 29, no. 6, pp. 1408-1415, 2013.

[10] J. Zhao, J. Tao, M. Stuempert, M. Post, "Combining cloud and grid with the user interface," in *Cloudcomp2009*, LNICST 34, pp. 103-111, 2010.

[11] Md. T. Khorshed, A. B. M. Shawkat Ali, S. A. Wasimi, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," *Future Generation Computer Systems*, vol. 28, no. 6, pp. 833-851, 2012.

[12] R. Buyya, C. S. Yeo, S. Venugopal, "Market-oriented cloud computing: vision, hype, and reality for delivering it services as computing utilities," *in 10th IEEE International Conference on High Performance Computing and Communications (HPCC '08)*, pp. 5 –13, Sept. 2008.

[13] D. Catteddu, G. Hogben, "Cloud computing: Benefits, risks and recommendations for information security," *Communications in Computer and Information Science*, vol. 72, pp. 17, 2010.

[14] P. Mell, T. Grance, "The NIST definition of cloud computing," *National Institute of Standards and Technology*, vol. 53, no. 6, 2009.

[15] G. Brunette, R. Mogull, "Security guidance for critical areas of focus in cloud computing V2. 1. 2009 CSA (cloud security alliance)," USA, Disponible en: http://www.cloudsecurityalliance.org/guidance/csaguide, v2.1, 1.

[16] D. Teneyuca, "Internet cloud security: The illusion of inclusion," *Information Security Technical Report* 3-4 (16), pp. 102-107, 2011.

[17] J. Archer, A. Boehm, "Security guidance for critical areas of focus in cloud computing V 3.0, Cloud Security Alliance" (2011).

[18] NIST, 2011, "NIST cloud computing program retrieved" 21 May 2011, from http://www.nist.gov/itl/cloud/.

[19] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1-11, 2011.

[20] C. Vazquez, E. Huedo, R.S. Montero, I.M. Liorente, "On the use of clouds for grid resource provisioning," *Future Generation Computer Systems*, vol. 27, no. 5, pp. 600-605, 2011.

[21] S. Srinivasamurthy, D. Liu, "Survey on cloud computing security," 2010.

[22] S. M. Habib, S. Hauke, S. Ries, M. Muhlhauser, "Trust as a facilitator in cloud computing: a survey," *Journal of Cloud Computing: Advances, Systems and Applications*, pp. 1-19, 2012.

[23] P. Srivastava, S. Singh, A. A. Pinto, S. Verma, V. K. Chaurasiya, R. Gupta, "An architecture based on proactive model for security in cloud computing," in *IEEE International Conference on Recent Trends in Information Technology*, pp, 661-666, 2011.

[24] www.rickscloud.com/top-threats-for-cloud-computing/

[25] J. Archer, A. Boehme, D. Cullinane, P. Kurtz, N. Puhlmann, J. Reavis, "Top threats to cloud computing," ver. 1.0. *cloud security alliance*, May 2010. (http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf).

[26] A. Sirisha, G. G. Kumari, "API access control in cloud using the role based access control model," in *Trend in Information Sciences & Computing (TISC'2010)*, pp. 135-137, 2010

[27] T. Andrei, R. Jain, "Cloud computing challenges and related security issues, a survey paper," 2009, DOI: http://www.cse.wustl.edu/~jain/cse571- 09/ftp/cloud.pdf.

[28] J. Spring, "Monitoring cloud computing by layer," *IEEE Security & Privacy*, vol. 9, no. 2, pp. 66–68, 2011.

[29] B. Grobauer, T. Walloschek, E. Stöcker, "Understanding cloud-computing vulnerabilities," *IEEE Security and Privacy*, vol. 9, no. 2, pp. 50-57, 2011.

[30] F. Lombardi, R. Di Pietro, "Secure virtualization for cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1113-1122, 2011.

[31] J. Li, B. Li, T. Wo, C. Hu, J. Huai, L. Liu, K. P. Lam, "Cyber Guarder: A virtualization security assurance architecture for green cloud computing," *Future Generation Computer Systems*, vol. 28, no. 2, pp. 379-390, 2012.

[32] K. Dahbur, B. Mohammad, A.B. Tarakji, "A survey of risks, threats and vulnerabilities in cloud computing," 2011.

[33] A. G. Revar, M. D. Bhavsar, "Securing user authentication using single sign-on in cloud computing," *IEEE International Conference Nirma University* (2011).

[34] S. Srinivasamurthy, D. Liu, "Survey on cloud computing security," 2010.

[35] D. W. Chadwick, K. Fatema, "A privacy preserving authorization system for the cloud," *Journal of Computer and System Sciences*, vol. 78, no. 5, pp. 1359-1373, Sept. 2012.

[36] M. Zhou, Y. Mu, W. Susilo, J. Yan, L. Dong, "Privacy enhanced data outsourcing in the cloud," *Journal of Network and Computer Applications*, vol. 35, no. 4, pp. 1367-1373, 2012.

[37] M. Mackay, T. Baker, A. Al-Yasiri, "Security-oriented cloud computing platform for critical infrastructures," *Computer Law & Security Review*, vol. 28, no. 6, pp. 679-686, 2012.

[38] C. Rong, S. T. Nguyen, M. G. Jaatun, "Beyond Lightning: A survey on security challenges in cloud computing," *Computers and Electrical Engineering*, vol. 39, no. 1, pp. 47-54, Jan. 2013.

[39] S. K. Sood, "A combined approach to ensure data security in cloud computing," Journal of Network and Computer Applications, vol. 35, no. 6, pp. 1831-1838, 2012.

[40] M. Noureddine, R. Bashroush, "An Authentication Model towards Cloud Federation in the Enterprise," The Journal of Systems and Software, vol. 86, no. 9, pp. 2269-2275, Sept. 2013.

[41] P. Prasad, B. Ojha, R.R. Shahi, R. Lal, "3-dimentional security in cloud computing," *in 3rd International Conference on Computer Research and Development (ICCRD, 2011)*, pp. 198-208, 2011.

[42] http://www.soasta.com/products/cloudtest-lite/.

[43] R. N. Calheiros, R. Ranjan, A. Beloglazov, C. A. F. De Rose, R. Buyya, "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms," *Software – Practice And Experience*, vol. 41, pp: 23–50, 2011.

[44] http://www.cloudbus.org/cloudsim

Masoumeh Zareapoor is a researcher in Department of Computer Science. Hamdard University, New Delhi, India. She received her PhD and M.Sc degree in Computer Science. Her research interest includes Data Mining, Machine Learning Cloud Computing, Intrusion Detection System, Artificial Intelligent and pattern recognition. She is member of Reviewer board of several Journals.

Pourya Shamsolmoali is a researcher in Computer Science Dept. Hamdard University, New Delhi, India. He received his M.Sc degree in Computer Science. His research interest includes Distributed System, Network system, Network Security, Mesh network, Cloud and Grid Computing, Middleware, Data Mining, Machine Learning and Intrusion Detection System

M. Afshar Alam is a Professor in Computer Science; he was Head of Computer Science Department, Faculty of Management and Information Technology, at the Hamdard University, New Delhi, India. In 1997-2000, he founded the Department of Computer Science, Hamdard University. He was also founder of Computer Centre at Hamdard University. He received his Master degree in Computer Science from the Aligarh Muslim University and Ph.D. from Jamia Millia Islamia University. His research interests include Fuzzy logic, Software engineering, Networking, Network Security, Cloud Computing and Bioinformatics. He is the author of a book on Software re-engineering and over 60 publications in International/ National journals, conference and chapter in an edited book. He is a member of expert committee AICTE, DST, UGC and Ministry of Human Resource Development (MHRD), New Delhi, India.

Guide for Authors
International Journal of Electronics and Information Engineering

International Journal of Electronics and Information Engineering (IJEIE) will be committed to the timely publication of very high-quality, peer-reviewed, original papers that advance the state-of-the art and applications of Electronics and Information Engineering. Topics will include, but not be limited to, the following: Algorithms, Bioinformatics, Computation Theory, AI, Fuzzy Systems, Embedded Systems, VLSI/EDA, Computer Networks, Information Security, Database, Data Mining, and Information Retrieval, Digital Content, Digital Life, and Human Computer Interaction, Image Processing, Computer Graphics, and Multimedia Technologies, Information Literacy, e-Learning, and Social Media, Mobile Computing, Wireless Communications, and Vehicular Technologies, Parallel, Peer-to-peer, Distributed, and Cloud Computing, Semiconductor, Software Engineering and Programming Languages, Telecommunication, etc.

1. Submission Procedure

Authors are strongly encouraged to submit their papers electronically by using online manuscript submission at http://ijeie.jalaxy.com.tw/.

2. General

Articles must be written in good English. Submission of an article implies that the work described has not been published previously, that it is not under consideration for publication elsewhere. It will not be published elsewhere in the same form, in English or in any other language, without the written consent of the Publisher.

2.1 Length Limitation:

All papers should be concisely written and be no longer than 30 double-spaced pages (12-point font, approximately 26 lines/page) including figures.

2.2 Title page

Title page should contain the article title, author(s) names and affiliations, address, an abstract not exceeding 100 words, and a list of three to five keywords.

2.3 Corresponding author

Clearly indicate who is willing to handle correspondence at all stages of refereeing and publication. Ensure that telephone and fax numbers (with country and area code) are provided in addition to the e-mail address and the complete postal address.

2.4 References

References should be listed alphabetically, in the same way as follows:

For a paper in a journal: M. S. Hwang, C. C. Chang, and K. F. Hwang, ``An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445--446, 2002.

For a book: Dorothy E. R. Denning, *Cryptography and Data Security*. Massachusetts: Addison-Wesley, 1982.

For a paper in a proceeding: M. S. Hwang, C. C. Lee, and Y. L. Tang, ``Two simple batch verifying multiple digital signatures," in *The Third International Conference on Information and Communication Security (ICICS2001)*, pp. 13--16, Xian, China, 2001.

In text, references should be indicated by [number].

2.5 Author benefits

No page charge is made.

Subscription Information

Individual subscriptions to IJEIE are available at the annual rate of US$ 200.00 or NT 6,000 (Taiwan). The rate is US$1000.00 or NT 30,000 (Taiwan) for institutional subscriptions. Price includes surface postage, packing and handling charges worldwide. Please make your payment payable to "Jalaxy Technique Co., LTD." For detailed information, please refer to http://ijeie.jalaxy.com.tw or Email to ijeieoffice@gmail.com.