Money Generation By Utilizing Idle Time Of Computers Through Innovative Cloud Storage Outsourcing

S.Rajkumar[1] M.Sai Anand[2] Vigneshwar Suresh[3]
rajkumar.df54@gmail.com msaianand@gmail.com vssvicky@gmail.com
Easwari Engineering College,Chennai,India

Abstract—— **Have you ever imagined that a computer at home or office can generate huge passive income despite being idle all the time? Computing powers are growing today enormously but its resources are not utilised to the fullest capability. We introduce a way that in which each and every computer in this world is used to its fullest capability but at the same time none of your day-to-day activities on the computer gets affected and also it generates huge income doing absolutely nothing extra. We propose the concept of cloud outsourcing for this i.e. we introduce a normal home/office user's system into Infrastructure-as-a-Service(IaaS) layer of the cloud architecture and so the idle time of the computers can be now used to save the world through this innovative idea. This idea would lead the cloud storage capacity of the world by many folds and that too at a very affordable price.**

I. INTRODUCTION

Cloud computing grew out of our never-ending hunger for ever-faster and ever-cheaper computation. The key driving forces behind it are the promise of broadband and wireless networking, lower storage and mobile device costs, and progressive improvements in Internet computing software and mobile computing.

Embracing cloud computing's growth and challenges, several companies have built high-performance systems (For example, Google's Bigtable) and Internet applications such as search, social networks, content delivery, collaborative software development, and online games and e- commerce applications.

The Pew Research Canter's Internet and American Life Project and Elon University recently conducted a survey of 900 Internet practitioners, social analysts, and researchers; their survey results confirm this viewpoint. Specifically, most of the survey respondents believe that Internet users will "live mostly in the cloud" by 2020.

The U.S. government expects that the annual growth rate of its spending on cloud computing will be about 40% in the 2010-2015,

Also, a recent Market Research Media study forecasts that "Cloud computing will enter an explosive growth phase — at about 40% compound annual growth rate — over the next six years and expenditure across the world will pass $7 billion by 2015."

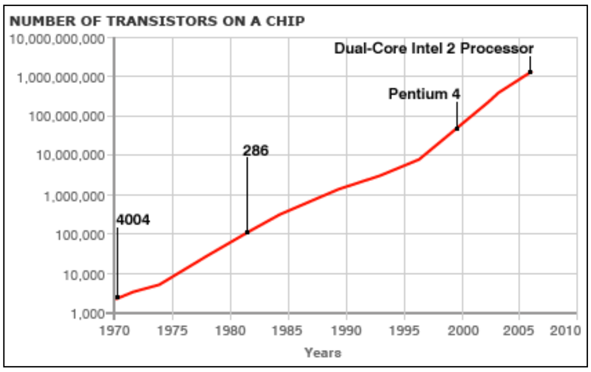
But Cloud technologies and models have not yet received their full potential, and many of the capabilities associated with clouds are not yet developed and researched to a degree that allows their exploitation to the full degree, respectively meeting all potential circumstances of usage.

Many people argue that we're moving from cloud 1.0 to cloud 2.0. Although it's too early to speak about the next cloud generation, its evolution will integrate Web 2.0 social networking features and functionality into cloud-based applications so that the cloud services are used to its fullest potential.

In this context, social cloud is another emerging trend in which users can discover and trade storage and computing services contributed by their friends in an online social network (for example, Facebook), taking advantage of pre-existing trust relationships.

II. MOORE'S LAW

According to Wikipedia, *Moore's law* is the observation that "the number of transistors in a dense integrated circuit has doubled approximately every two years". The observation is named after Gordon E. Moore, the co-founder of Intel and Fairchild Semiconductor, whose 1965 paper described a doubling every year in the number of components per integrated circuit, and projected this rate of growth would continue for the upcoming decades.



The idea of this paper is made having Moore's Law as one of its pillars. Though computational powers are increasing day by day, it is not used to its fullest and is getting wasted. For instance, today a school kid uses a computer as powerful as used by a professor at Harvard or maybe even one of those used for research purposes at Cambridge. But the key point is that, the usage of the computers in both cases are not going to be the same. In other words, a lot of computing power remains unused in the kid's computer. Today in many leading firms, we observe that a lot of computers are being used 24x7 and also they are provided with a stable high speed internet connection. But most of the time they remain idle and the hard drives are not fully utilised. We thus propose an idea to use this empty space and computer idle time to its fullest use through cloud outsourcing.

III. PROPOSED WORK

Through cloud outsourcing we tend to make office and home computers as *money generators* rather than just *output generators* for your queries. A recent survey by the Elon University shows that the average home user uses only 22% of the total resources available on the computer.

For instance , Suppose you have a computer powered with Intel®Core™2 Duo E8190 Processor clocked at 2.66 GHz ,1 TB hard drive and a 8GB RAM its quite natural that that a normal office or home user would be using all the available power.

Let us consider about 300 GB and 4GB of RAM is used up for the office/home works. Then the remaining space and RAM space is left free and unused. In that case, the empty space is rented to the big cloud merchants like Google Drive, Microsoft OneDrive, etc. so that they can use your device as a part of their cloud without any of your activities getting affected. And also the companies which are using your system will pay you accordingly. So the computers become passive money generators with absolutely the user doing nothing extra.

Statistics say Google get 90% of its revenue from advertising and they are spending about 56% of their wealth on cloud services maintenance and development.

The company willing to rent storage spaces from the normal office and home systems first checks it availability i.e. its 24x7 connectivity , security ,and a series of other tests, and then locks a space in the system for cloud storage. The information stored is encoded. A firewall is also designed so that the user cannot view the stored information of cloud and also the people who access the cloud cannot view the user's information in the local system.

The agreement can be done online and the duration could be for a month, a quarter, half or even a full year. And the rental amount shall be payable directly to customer's bank account through the secured payment channels.

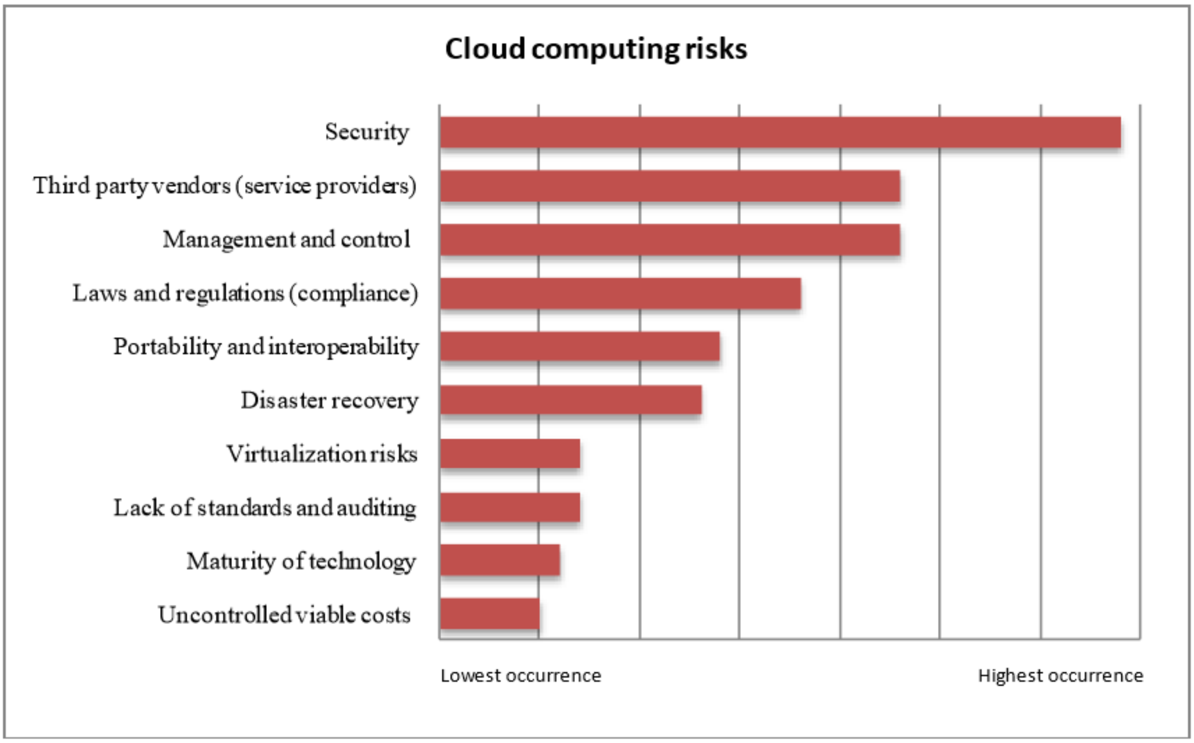
So by this we understand that cloud outsourcing to the normal users can be a win-win situation in which both ends can be met without disturbing any of the other activities of both the provider and the client.

A normal server bought for extra cloud storage by a company would cost way higher than the money spent for this rented storage from the user. By implementing this, the overall cost of acquiring extra storage space for the cloud system would increase by an estimated massive 350% and at the same time with cost efficiency of 400%.

IV. USES OF CLOUD OUTSOURCING

Using a cloud provider, companies can start small and increase hardware resources only when necessary. This eliminates the need to plan far ahead for provisioning computing resources. Start-up companies who cannot afford large servers for their cloud storage can use this idea to get the same cloud benefits at a lower cost.

In academia, college students use the cloud infrastructure to develop their skills and build next-generation computing infrastructures and applications. All this advocates that this discipline has a prosperous future and will become one of the most significant industries.



V. RISKS IN OUTSOURCING

Even though there is a very large scope for this cloud based solution, cloud computing is not without risks or completely secure. A thorough understanding and the mitigation of security risks represent an important step towards securing cloud environments and harnessing the benefits of cloud computing. The first step in our research was to review the published literature and to conduct an analysis to identify the risks.

According to the literature review, the biggest cloud computing concern is security. With applications and data being hosted by a service provider, data is no longer under the control of management and prone to vulnerabilities. Hosting application and data in shared infrastructures increase the potential of unauthorised access and raise concerns such as privacy, identity management, authentication, compliance, confidentiality, integrity, availability of data, encryption, network security and physical security.

Apart from the security risks, other concerns include third-party (service provider) management, vendor lock-in, quality of service, vendor viability, data and application management and control, workload management, performance, change control, availability of service, the lack of monitoring and management tools, transparency, compliance with laws and regulations, portability and interpretability, disaster recovery, virtualization risks, the lack of standards and auditing, the unproven nature of cloud computing and uncontrolled viable costs.

Information security was rated by 91.7 % of the respondents to be the most critical risk area for the implementation of cloud computing and virtualization standards, policies and controls. Disaster recovery / business continuity planning was rated the second most critical risk area, with a score of 66.7 %.

The findings from the literature survey corroborate the importance of ensuring that the cloud environment is adequately protected and secure. Establishing controls to overcome the security issues are hence an important step towards securing the cloud environment that are to be stored in the local systems of the users. We therefore focus primarily on security risks when we discuss risk mitigation strategies in the remainder of the paper.

VI .MITIGATION OF SECURITY RISKS

Through the extensive literature review, the following control objectives were identified as important for the mitigation of cloud computing security risks: data security, administration and control; logical access; network security; physical access; compliance; and virtualization. Each of these objectives is discussed in more detail in the following sections.

Most of the security risks and subsequent controls, described in the remainder of this paper, constitute resources being hosted by a service provider at an off-site location, regardless whether it is a public cloud, private cloud, community cloud or a combination of two or more clouds

A. Data security, administration and control:
Data security risks constitute the biggest barrier for cloud computing. Some businesses are still reluctant to move data and applications to the rental cloud proposed in the paper, especially if critical to the business, due to the risk of data leakage leading to confidentially and privacy risks, the lack of control over hosted data and applications, availability concerns of cloud services and data, the risk of data integrity impairment, and ineffective protection of data in transit, in rest or in back-up due to inadequate encryption.

B. Logical access:
Access via a public network and hosted services means increased exposure and subsequently more risks. Privileged access rights should be assigned carefully to authorised users only, and reviewed for adequacy on a frequent basis. The implementation of security tools and techniques are required to ensure authorised user access to data and applications.

C. Network security:
Network security risks include the increased risk of hacking and intrusion, enterprise perimeter evaporation and mobile device attacks.

D. Physical security:
With the disappearance of physical data centre perimeters, attackers could gain access to data and applications from anywhere in the network.

E. Compliance:
Companies are ultimately responsible for ensuring the security and integrity of their data, even when it is held by service providers in the cloud. Organisations further need to prove compliance with security standards regardless of the locations of their data and applications.

F. Virtualization:
In previous research we have addressed virtualization security risks and a number of controls that could be considered for the mitigation of virtualization security risks. The controls included those related to security administration and control, logical access, network security, physical security, change control, and management and monitoring.

VII. RISK MANAGEMENT AND SUCCESSFUL IMPLEMENTATION TECHNIQUES

To truly implement this idea of outsourcing cloud computing, we need to gradually improve it in academic, legal and institutional and take into consideration each of the risk factors specified above. Especially, the issue of trust is one of the biggest obstacles for the development of proposed idea. In this idea, there is a need mutual trust of the users and the services providers, and neither is dispensable.

For instance, because user lacks controllability of data, equipment and environmental, which lead to mistrust of cloud computing, include: data disclosure risk, store location security risk, data being investigated risk, data loss risk, service interruptions and the cloud provider collapse, unauthorised and improper bank transactions during the payment stage, there are a lot of challenges involved in this idea.

In the cloud computing, the first user trust is the user's identity trust, but we only have the user identity trust in the cloud which is not enough, the issue of user behaviour trust also must be evaluated and managed. Traditional authorization and authentication may solve the issue of user's identity trust, but does not solve the problem of trust on user's behaviour.

Hence we provide a list of ways in which the trust in between the provider and the user both ways for the success of this proposal.

VIII. EVALUATION PROCESS FOR CHOOSING TRUSTABLE USERS TO RENT CLOUD

We introduce a term called trust value to rate the users whose behaviour and thereby use the rating to extend/cancel the agreement

• *Slow-rise:*
Trust and risk is a pair of contradictory unity, so we need to guard against the risk even of that we have high trust each other. *Slow rise* is a strategy that is to prevent the user immediately get a high storage value immediately after the agreement is signed. Initially a small space is taken and based upon the performance of the user system the rented storage is increased in small steps and the trust value is incremented on each successful testing.

• *Rapid-decline:*
In case of any cheating rapid decline is an evaluation strategy to punish non-trust behaviour afterwards.

The overall trust value of user that was rated mistrustful in any time will be quickly reduced. The intensity of the reduced trust value is far greater than that gradually increased when finding cheating behaviour, which can prompt the user to reduce fraud, and the rented storage is decreased rapidly.

• *Double Sliding Window:*
This technique is used to evaluate the user system’s performance rather than behaviour. Based on the basic criteria of the evaluation, we decide the sliding window to carry out the evaluation of node behaviour trust. In that, the trust value not only with the time related, but also with m the number of actual contacts about nodes in the window, and the window's size which control evaluation scale. And also the enough (sliding window size) original evidences were retained, in order to share the trust information or re-evaluate the trust for different needs. The movement of window is involved with two factors: the time t and the new node intercourse. As time goes by, the window moves forward, and then some overdue trust records gradually out of the window. In this way, we can ensure that the overall trust value of the node will be decreased when the node doesn't exchange information with others in a long time. When a new intercourse comes, and the window size is fixed, so the record which has the farthest time from the current and wasn't overdue was "squeezed out" thought the window's movement. In this way, we can achieve the goal that the trust evaluation is scalability. Based on the background of actual application on WSNs, by selecting the model factors: the trust effective time period, the window size etc. and updating the window content, it not only effectively control the nodes of deception and punish fraud, but also the algorithm has good scalability. In computing user behaviour trust of effective trust records within windows, the basic idea of calculation is that the more recent, the more abnormal behaviour has the greater proportion of comprehensive evaluation, the degree of abnormal behaviour is shown by the standard variance of history trust d, the proportion which each trust for overall trust varies with the record time, where d is a scale factor which between the behaviour time with the behaviour abnormal.

IX. TESTING PROCESS OF IMPLEMENTED CLOUD

Cloud-based software testing refers to testing and measurement activities on a cloud-based environment and infrastructure by leveraging cloud technologies and solutions.

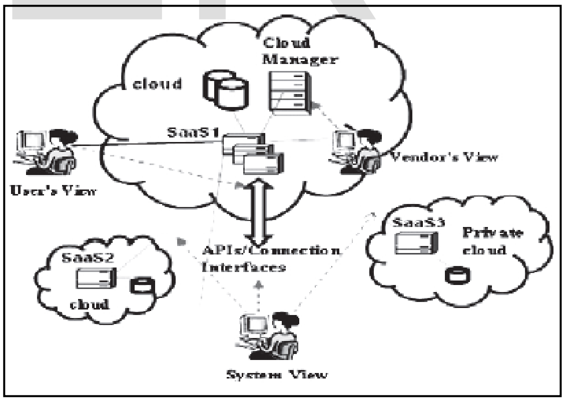
There are four different forms of cloud-based software testing. Each of them has different focuses and objectives.

• *Testing a XaaS in a cloud:*
It assures the quality of everything as services (XaaS) in a cloud based on its functional and non-functional service requirements.

• *Testing of a cloud* :
It validates the quality of a cloud from an external view based on the provided cloud specified capabilities and service features. Cloud vendors as well as end users are interested in carrying on this type of testing.

• *Testing inside a cloud*:
It checks the quality of a cloud from an internal view based on the internal infrastructures of a cloud and specified cloud capabilities. Only cloud vendors can perform this type of testing since they have accesses to internal infrastructures and connections between its automatic capabilities, and security management.

• *Testing over clouds:*
It tests cloud-based service applications over clouds, including private, public, and hybrid clouds based on system level application service requirements and specifications. This usually is performed by the cloud-based application system providers.



In a cloud environment, the first is the vendor view, which presents the testing view from the engineers of a cloud vendor. They perform vendor-oriented software testing tasks. The next is the user view, which presents the consumer-oriented testing view from cloud-based application users through web-based user interfaces. They conduct testing and QA jobs to assure the of provided application services in a system-oriented test view in a given cloud infrastructure where different cloud based Applications may interact with each other. They need to perform different testing tasks to assure the quality of the cloud-based application systems over clouds, such as cloud-based application integration, end-to-end system function testing, system performance and scalability over different clouds.

X. PAYMENT METHODS TO THE USER

Today the potential of cloud computing is so high that even banking is performed with help of clouds. Thus it is very easy to implement all the payment to be made to the users.

The *AlphaHubCloud* consolidates the payments world onto one platform enabling Banks, Merchants, MSPs and ISOs to access any payment type, any solution provider, anywhere in the World.

XI. CONCLUSION

Cloud computing is the key to the world's development in the modern age. To make cloud computing more accessible and available at affordable rates, we have given a win-win solution that benefits both the vendor and the user. We provided an overview of cloud outsourcing benefits and security risks as a general guideline to assist management in the implementation of cloud outsourcing and renting processes, procedures and controls. Consideration should be given to risks to ensure completeness, integrity and availability of applications and data in the cloud. We have also suggested a number of controls that could be considered for the mitigation of cloud computing security risks. The controls included data security, administration and control, logical access, network security, physical security, compliance and virtualization. Further research will focus on the implementation of the idea across the globe and also on the development of a complete risk and control framework for cloud outsourcing and virtualization to provide management with guidelines and control standards.

XII. REFERENCES

[1] Deloitte. (2010, 31 August 2010). *Executive Forum - Cloud Computing: risks, mitigation strategies, and the role of Internal Audit*. Available: http://www.deloitte.com

[2] C. Pettey and B. Tudor. (2010, 5 August 2010). *Gartner says worldwide cloud services market to surpass $68 billion in 2010* Available: http://www.gartner.com/it/page.jsp?id=1389313

[3] Press Office. (2010, 31 August 2010). *Cloud Computing Services - New Market Report Published*. Available: http://www.companiesandmarkets.com/r.ashx?id=41AETZYHJ289173&prk=ecb8413c602cb89051067456b636c7b9

[4] I. Berger. (2010, 6 May 2010). *Keeping Cloud Computing's Prospects Safe and Sunny*. Available: http://www.theinstitute.ieee.org/portal/site/tionline/menuitem.130a3558587d56e8fb2275875bac26c8/index.jsp?&pName=institute_level1_article&TheCat=2201&article=tionline/legacy/inst2010/may10/featuretechnology.xml&

[5] K. McCabe and R. Nachbar. (2010, 18 October 2010). *SURVEY BY IEEE AND CLOUD SECURITY ALLIANCE DETAILS IMPORTANCE AND URGENCY OF CLOUD COMPUTING SECURITY STANDARDS* Available: http://standards.ieee.org/announcements/2010/pr_cloudcomputing_survey.html

[6] Centre for the Protection of National Infrastructure (CPNI). (2010, 20 June 2010). *Information Security Briefing 01/2010: Cloud Computing*. Available: http://www.cpni.gov.uk/Docs/cloud-computing-briefing.pdf

[7] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Information Technology Laboratory2009.

[8] S. Baca. (2010, 14 May 2010). *Cloud Computing: What it is and what it can do for you*. Available: www.globalknowledge.com

[9] S. Bennett*, et al.* (2009, 8 April 2010). *Architectural Strategies for Cloud Computing*. Available: http://www.oracle.com/technology/architect/entarch/pdf/architectural_strategies_for_cloud_computing.pdf

[10] Cloud Computing Use Case Discussion Group. (2010, 31 March 2010). *Cloud Computing Use Cases Version 3.0.* Available: http://groups.google.com/group/cloud-computing-use-cases

[11] Sun Microsystems Inc. (2009, 8 April 2010). *Introduction to cloud computing architecture* [White Paper]. Available: http://www.sun.com/featured-articles/CloudComputing.pdf

[12] VMware Inc. (2009, 18 August 2010). *Eight Key Ingredients for Building an Internal Cloud*. Available: http://www.vmware.com/files/pdf/cloud/eight-key-ingredients-building-internal-cloud.pdf

[13] Cloud Security Alliance. (2009, 20 May 2010). *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.*

[14]Images and other contents http://www.google.com

[15]Contents from http://www.wikipedia.com

[16] M. Armbrust et al., *"A View of Cloud Computing," Comm. ACM*, vol. 53, no. 4, 2010, pp. 50–58.

[17] M.D. Dikaiakos et al., *"Cloud Computing: Distributed Internet Computing for IT and Scientific Research," IEEE Internet Computing, vol. 13, no. 5, 2009, pp. 10–13.*