CERTIFIABLE STATEMENT SYSTEM FOR SECURE CLOUD COMPUTING

T VENKATESHWARA REDDY 1*, E RAVI 2*

1. *M.Tech – Student, Dept of CSE, KHADER MEMORIAL CET, Devarakonda, Nalgonda, Telangana.*
2. *Asst. Prof, Dept of CSE, KHADER MEMORIAL CET, Devarakonda, Nalgonda, Telangana.*

Abstract— The utilization of cloud computing resources as PaaS(Platform as a Service) has widely increased due to which the security issues had become highly captious. The billing system in the cloud does not articulate the security credentials and is not efficiently immune. The existing billing system generates a onetime password which could also be hacked via a hacker and the system is vulnerable to attack. In this paper, we propose a competent and a solitude billing system. The system uses a cloud notary authority (CNA) which monitors the billing agent. The geographic location information of the user traced by the cloud notary authority is for the fraudulent detection. It also generates a certification code (CFC) to scrutiny the intrusion. The CNA binds the CFC code and the geo-location to provide a highly secured and an integrated system. The performance evaluation of this system is better than the PKI (public key infrastructure).

***Index Terms*—Computing, cloud computing, One time password, Cloud notary authority, Certification code, Public key infrastructure.**

1.INTRODUCTION

Cloud computing is an emerging technology and is the overgrowing trend in an IT environment. As a metaphor for the Internet, "the cloud" is a familiar cliché, but when combined with "computing," the meaning gets bigger and fuzzier. Cloud computing comes into focus only when you think about what IT always needs: a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software.

Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends IT's existing capabilities. Major models of cloud computing service are known as software as a service, platform as a service, and infrastructure as a service. These cloud services may be offered in a public, private or hybrid network. A cloud can be private or public. A public cloud sells services to anyone on the Internet. (Currently, Amazon Web Services is the largest public cloud provider).A private cloud is a proprietary network or a data canter that supplies hosted services to a limited number of people. When a service provider uses public cloud resources to create their private cloud, the result is called a virtual private cloud. Private or public, the goal of cloud computing is to provide easy, scalable access to computing resources and IT services.

Cloud service providers (CSPs) generally use a pay-per-use billing scheme in their pay-as-you-go pricing model. It usually guarantees the quality of service in the form of a service level agreement (SLA). An SLA is supported by regular performance monitoring. In this IaaS can be utilized by enterprise customers to create cost effective and easily scalable IT solutions where the complexities and expenses of managing the underlying hardware are outsourced to the cloud provider.

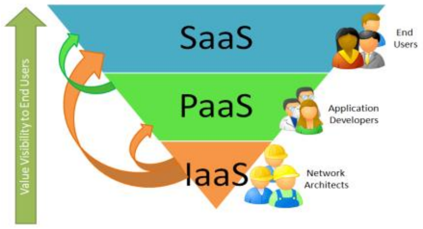


Figure 1 Services of cloud computing

Figure 1 shows that the important services of cloud computing .SaaS is a Access to Software as a Service which is compatible across all internet enabled devices.PaaS facilitates deployment of cloud-based applications without the cost of buying and maintaining the underlying hardware and software layers . As with SaaS and IaaS, PaaS depends on a secure and reliable network and secure web browser. PaaS application security comprises two software layers: Security of the PaaS platform itself (i.e., runtime engine), and Security of customer applications deployed on a PaaS platform . PaaS providers are responsible for securing the platform software stack that includes the runtime engine that runs the customer applications. If the company uses PaaS as a service then it has to keep its application in a more secured manner. Users account has to be verified and must be integrated.

Using a cloud computing service can mean greater server and compute capacity when you need it and without the costs and management headaches of owning all the hardware. Public cloud computing services, in particular, offer easy and inexpensive set-up, a pay-per-usage model and the scalability needed to meet specific needs. Google, Amazon, Oracle Cloud, Sales force, Zoho, and Microsoft Azure are some well-known cloud vendors.[1,2]

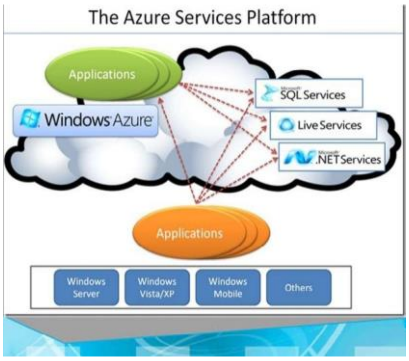


Figure 2 Azure services platform

In this paper we have used Microsoft azure because of its low cost, and easily access without online for some applications. Azure services platform as shown in Fig(2).

Microsoft Azure comes with a range of free options for its popular services. You can deploy up to 10 free web sites, or build a mobile service that supports up to 500 devices, without having to pay a penny. Both options come with some storage (though that part is only free for a year) and seem tailored for small development teams and for small projects. You can use the free mobile service option to build the backend for an app, without impacting your company's network and server resources, and then if it proves successful, transition it to either a paid tier or to your own internal servers. If you're a start up access is also available as a benefit to organizations and you're not limited to using Microsoft technologies, as

There's support for Linux virtual machines on Azure's IaaS service.

2. SECURITY ISSUES IN CLOUD COMPUTING

Cloud security issues and the risks of cloud computing are not well understood today and are one of the biggest barriers to adoption of these services.

While security and privacy concerns when using cloud computing services are similar to those of traditional non-cloud services, concerns are amplified by external control over organizational assets and the potential for mismanagement of those assets. Transitioning to public cloud computing involves a transfer of responsibility and control to the cloud provider over information as well as system components that were previously under the organization's direct control. The transition is usually accompanied by loss of direct control over the management of operations and also a loss of influence over decisions made about the computing environment.

Despite this inherent loss of control, the cloud service consumer still needs to take responsibility for their use of cloud computing services in order to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security and privacy that are in the best interest of the organization. The consumer achieves this by ensuring that the contract with the provider and its associated service level agreement (SLA) has appropriate provisions for security and privacy. In particular, the SLA must help maintain legal protections for privacy relating to data stored on the provider's systems. The consumer must also ensure appropriate integration of the cloud computing services with their own systems for managing security and privacy.

Cloud computing represents a very dynamic area at the present time, with new suppliers and new offerings arriving all the time. There are a number of security risks associated with cloud computing that must be adequately addressed: [2]

- *Loss of governance.*

For public cloud deployments, consumers necessarily cede control to the cloud provider over a number of issues that may affect security. At the same time, cloud service level agreements (SLA) may not offer a commitment to provide such capabilities on the part of the cloud provider, thus leaving gaps in security defenses.

- *Responsibility ambiguity*

Given that use of cloud computing services spans across the consumer and the provider organizations, responsibility for aspects of security can be spread across both organizations, with the potential for vital parts of the defenses to be left unguarded if there is a failure to allocate responsibility clearly. The split of responsibilities between consumer and provider organizations is likely to vary depending on the model being used for cloud computing (e.g. Iaas versus SaaS).

- *Isolation failure*

Multi-tenancy and shared resources are defining characteristics of public cloud computing. This risk category covers the failure of mechanisms separating the usage of storage, memory, routing and even reputation between different tenants (e.g., so-called guest-hopping attacks).

- *Vendor lock-in*

Dependency on proprietary services of a particular cloud provider could lead to the consumer being tied to that provider. Services that do not support portability of applications and data to other providers increase the risk of data and service unavailability.

- *Data protection*

Cloud computing poses several data protection risks for cloud consumers and providers. The major concerns are exposure or release of sensitive data but also include loss or unavailability of data. In some cases, it may be difficult for the cloud consumer (in the role of data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g., between federated cloud services.

- *Insecure or incomplete data deletion*

Requests to delete cloud resources, for example, when a consumer terminates service with a provider, may not result in true wIPing of the data. Adequate or timely data deletion may also be impossible (or undesirable from a consumer perspective), either because extra copies of data are stored but are not available, or because the disk to be deleted also stores data from other clients. In the case of multi-tenancy and the reuse of hardware resources, this represents a higher risk to the consumer than is the case with dedicated hardware.

While the above security risks need to be addressed, use of cloud computing provides opportunities for innovation in provisioning security services that hold the prospect of improving the overall security of many organizations. Cloud service providers should be able to offer advanced facilities for supporting security and privacy due to their economies of scale and automation capabilities - potentially a boon to all consumer organizations, especially those who have limited numbers of personnel with advanced security skills.

3. THREATS AND COUNTERMEASURES IN CLOUD

There are some dangerous types of threats which are not specific to cloud environment, but lunched vastly in cloud systems due to the characteristics of cloud systems and their generality at present as shown in Figure 3.

- *SQL injection attacks*

In this type of attack a malicious code is inserted into a standard SQL code. Thus the attackers gain unauthorized access to a database and are able to access sensitive. For this type of threats need to use filtering techniques to sanitize the user input etc. are used to check the SQL injection attacks. A proxy based architecture towards preventing SQL Injection attacks which dynamically detects and extracts users' inputs for suspected SQL control sequences has been proposed in [5].

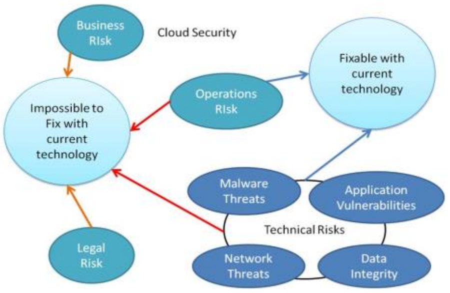


Figure 3 Security risks of cloud computing

- *Cross Site Scripting (XSS) attacks*

Injecting malicious scripts into Web is done in this kind of attack. There are two methods for injecting the malicious code into the web-page displayed to the user: Stored XSS and Reflected XSS. In a Stored XSS, the malicious code is permanently stored into a resource managed by the web application . However, in case of a Reflected XSS, the attack script is not permanently stored; in fact it is immediately reflected back to the user .For this kind of threats we have various techniques like: Active Content Filtering, Content Based Data Leakage Prevention Technology, Web Application Vulnerability Detection Technology has already been proposed to prevent XSS attacks [6]. These technologies adopt various methodologies to detect security flaws and fix them. A blueprint based approach that minimizes the dependency on web browsers towards identifying untrusted content over the network has been proposed in [7].

- *Man in the Middle attacks (MITM)*

In such an attack, an entity tries to intrude in an ongoing conversation between a sender and a client to inject false information and to have knowledge of the important data transferred between them. Various tools implementing strong encryption technologies like: Dsniff, Cain, Ettercap, Wsniff, Airjack etc. have been developed in order to provide safeguard against them. A few of the important points like: evaluating software as a service security, separate endpoint and server security processes, evaluating virtualization at the end-point have been done to tackle with this kind of attack in cloud computing [8]. In most of the cases, the security practices implemented (in the organization's private network) apply to the private cloud too. However, in case of a public cloud implementation, network topology might need to be changed in order to implement the security features [9].

- *Sniffer Attacks*

These types of attacks are launched by applications which can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted, it can be read. A sniffer program, through the NIC (Network Interface Card) ensures that the data/traffic linked to other systems on the network also gets recorded.

A malicious sniffing detection platform based on ARP (address resolution protocol) and RTT (round trip time) can be used to detect a sniffing system running on a network [10].

If a hacker is able to get control over the hypervisor, he can make changes to any of the guest operating systems and get control over all the data passing through the hypervisor [11]. Based on the understanding of how the various components in the hypervisor architecture behave, an advanced cloud protections system can be developed by monitoring the activities of the guest VMs (Virtual Machines) and inter-communication among the various infrastructure components [12, 13].

- *Denial of Service Attacks*

A DoS attack is an attempt to make the services assigned to the authorized users unavailable. In such an attack, the server providing the service is flooded by a large number of requests and hence the service becomes unavailable to the authorized user. Sometimes, when we try to access a site we see that due to overloading of the server with the requests to access the site, we are unable to access the site and observe an error. Usage of an Intrusion Detection System (IDS) is the most popular method of defense against this type of attacks [14]. A defence federation is used in [15] for guarding against such attacks. Each cloud is loaded with separate IDS. The different intrusion detection systems work on the basis of information exchange. In case a specific cloud is under attack, the cooperative IDS alert the whole system. A decision on trustworthiness of a cloud is taken by voting, and the overall system performance is not hampered.

4. ONE TIME PASSWORD

Every user is required a unique password for the authentication. As the password can be easily guessed or can be easily hacked, the onetime password is used. A one-time password (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. On the downside, OTPs are difficult for human beings to memorize. Therefore they require additional technology to work**.** As shown in fig.4,the user while the login session , an request of OTP is sent to the web server, from there the OTP is sent via a SMS gateway and the OTP is transferred to the mobile device. then the user logins through the received OTP ,which is validated for using the account.

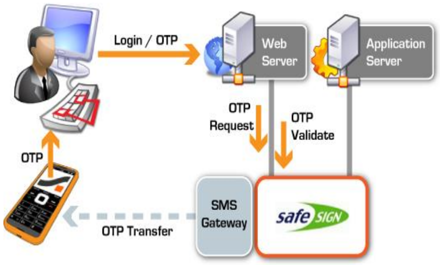


Figure 4 Method of generating one time password

In such conditions where security is the most essential issue, Providing a secured mechanism in a very trusted manner is critical for CSPs and users. However, the security aspects of a cloud system and the scale of cloud services while the usage of one time password, often raise the following security and system issues[3]

1. . There are many ways to generate OTPs, and a swarm of security companies have sprung up, each offering a different variant of One Time Password technology.

2. OTP is equally vulnerable because the action remains on the same device that the first layer of authentication occurs (username and password).For example, if a victim's computer is already vulnerable to key-loggers and other malware that can track what the victim is keying-in, and also take action based on the victim's activity, even a onetime password would fail. The following case scenario explains how the vulnerability occurs: The victim enters the username and password and clicks on the button to generate the one time password. The OTP either appears on a proprietary device or is sent as an SMS to their cell phone .The page where the victim has to enter first factor credentials is already being tracked and that information captured. Then the victim enters the OTP in the field provided and the malware detects this activity and then disconnects the victim. Before this, it has already captured both factors of authentication credentials. This information can now be used by the hacker to access the victim's account from another computer, and switch off the two factor authentication option as well as change the first factor credentials - the username and password. By the time all this happens and the victim connects and tries to sign in again, he cannot as his account has already been hijacked.

3. There are other social engineering attacks in which phishers steal OTPs by tricking customers into providing one or more OTPs that they used in the past scenarios that could do the same thing, such as if the victim receives a phone call before he clicks on the sign in button and is caused to move away from the computer, etc.

4. People who write sophisticated malware know a lot more tricks that can defeat what OTP security solutions offer.

5. Even time-synchronized OTPs are vulnerable to phishing, by two methods: The password may be used as quickly by the attacker as the legitimate user, if the attacker can get the OTP in plaintext quickly enough. The other type of attack—which may be defeated by OTP systems implementing the hash chain as discussed above—is for the phisher to use the information gained (*past* OTP codes which are no longer valid) by this social-engineering method to predict what OTP codes will be used in the *future.*

6. users of OTP systems are still vulnerable to man-in-the-middle attacks.[4]

A thorough investigation of existing method in various computing environments has helped us identify the above limitations in terms of security capabilities or computational overhead. To overcome these limitations, we propose a secure and no obstructive system. Specifically, we devised the following two mechanisms, which drive the architecture of our system.

1. Support more security: The transaction from a particular account is vulnerable to the intruder or to the unauthorized access, hence in our system we trace the Geographical location of the user for this the Google API key is used. The latitude and longitude co-ordinates are also traced and is stored.

2. Certification code generation: The intruder may use any network IP for the access of account of the user. The user may be unaware of this attack. Hence a code is generated which is known as certification code which certifies the current network IP of the user.

3. Enhanced and efficient OTP generation: Using both, the geographical location co-ordinates (i.e.) the latitude and longitude and the network IP, an OTP is generated which cannot be guessed or hacked by any intruder or any expert hacker.

5. CERTIFIABLE CODE (CFC)

- *Architecture*

Figure 5 shows an overview of the system, such a system can be used in any transaction oriented application. The CNA provides a mutually verifiable integrity mechanism that combats the malicious Behaviour of users or the CSP. The process, which involves a generation of mutually verifiable binding information among all the involved entities on the basis of a one-way hash chain, is computationally efficient for a thin client and the CSP.

Trusted SLA Monitor (S-Mon). The S-Mon has a Forgery-resistive SLA measuring and logging mechanism, Which enables it to monitor SLA violations and take corrective actions in a trusted Manner. After the service session is finished, the data logged by S-Mon are delivered to the CNA.

We devised S-Mon in such a way that it can be deployed as an SLA monitoring module in the computing resources of the user. We assume that users are thin clients who use the application in the cloud computing environment. To Start a service session in such an environment, each User makes a service check-in request to the CSP with a billing transaction. To end the service session, the user can make a service check-out request to the CSP with a billing transaction.

- *Transaction*

The registration in our system is done at the admin phase and the overall process is explained in a stepwise manner and they are as follows:

1. An account number and the password is generated by the admin and the password is encrypted using a cryptography technique.

2. The generated account number and password is sent to the user's emailID and their respective mobile number provided by the user during the registration phase.

3. The user can now login with the username provided and the password. During a login, a pseudorandom OTP will be generated and will be sent to the mobile device.

4. The user has to specify the received OTP to use their account for the transaction to continue.

5. While the transaction, the user has to click on the link, that link traces the location of the user.

6. After the above tracing process, the admin will generate an Opt that will b generated using the location and the network IP will be sent to the user via mobile and to the emailed.

7. If the user is not the one using the account can terminate the transaction by clicking on the cancel the transaction link.

- *Algorithm*

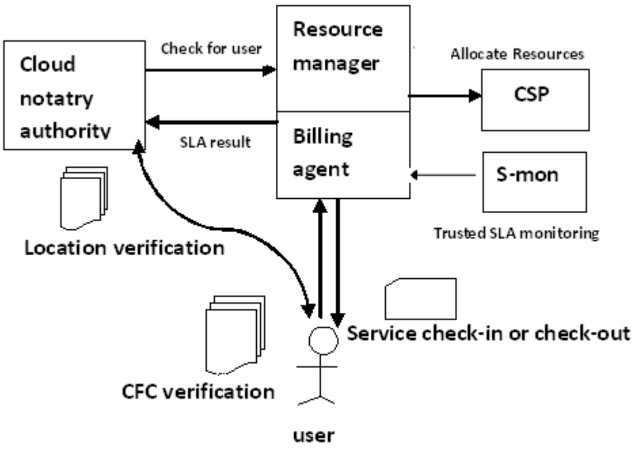


Fig5:Overall architecture of the proposed system

In this section, we describe the overall transactions of the Proposed billing scheme, , we analyse the Security and safety of the proposed billing system.

- *CFC Code Generation Algorithm*

```
INITIALIZE the transaction
Use results from LIVE-VARIABLE ANALYSIS, if available
Else, set all variables to L(0) -- LIVE after this block
Go through the instructions in REVERSE order...
FOR each instruction DO
Look up the current status of each variable (x, y1, y2, ...)
Fill in the NEXT-USE info for this instruction.
Set the status of “x” to “D”
Set the status of “y1
” to “L(n)”
Set the status of “y2
” To “L(n)”
ENDFOR
```

This algorithm checks for the live network of the user. It traces the network IP and stores it in a session. For each transaction, this network IP will be checked and will be saved in the session. So that it can check whether the ongoing transaction for the upcoming process or transactions from the same network IP or not .Each time the live variable has to be setup and the current status has to be checked. This will give a wide support while a transaction is ongoing and an intruder is trying to access our account from a different network IP.

- *Code Validation Algorithm*

```
Initialize REGISTER-DESCRIPTORS to “EMPTY.”
Initialize VARIABLE-DESCRIPTORS to in “MEMORY.”
FOR EACH IR Statement DO
Let x be the defined variable (if any).
Let y and z be the used variables (if any).
/*Comments */ (At this point, the REGISTER-DESCRIPTORS and VARIABLE-DESCRIPTORS tell what is in regs and where the variables are stored.) /*Comments */
Step 1:Determine where we will be storing the result value.
Call it “DEST”
Step 2:Move “y” into “DEST”.
Step 3:Figure out where “z” is.
Generate the instruction.
Step 4:Update REGISTER-DESCRIPTORS
 and VARIABLE-DESCRIPTORS.
```

```
END FOR
```

The above algorithm will validate the network IP generated that whether the transaction is from the same network IP or not. The information will be either stored in the memory or in the registers. The already traced network IP will be moved to the dest field, then for the next transaction that register will be updated for the further validation.

- *Location Trace back algorithm*

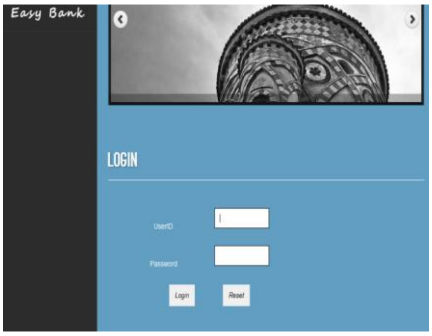
```
for each IPpacketw{
let x be a random number from [0, 1)
if (x<p) {
write n.ZoneID tow.zoneID;
w.distance = l;
}
else {
if ((w.zoneID != null)&&(w.zoneID != n.zoneID))
w.distance++;
}
}
forward IPpacketw;
```

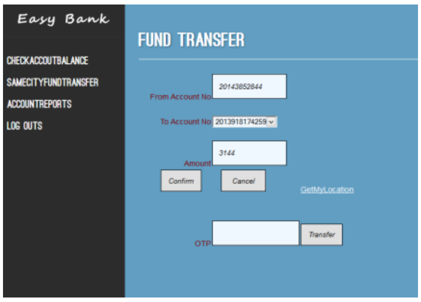
In the above algorithm, trace back determines the origin of a packet on the Internet. The packets with the IP address, analysis shows that in order to gain the correct attack path with accuracy. For each packets transferred coordinates corresponding to the zone id is fetched. If the Zone ID is not available the credentials used during the previous session is used to track the co ordinates. The process is repeated for each transaction and the session is maintained to further detections.

6. RESULTS AND DISCUSSION

In this section, we discuss additional issues, including an instance of actual deployment from the perspective of feasibility and additional extensibility, which may benefit from the security properties of our proposed system. We have shown the snap shots.

As a secured system is concerned, the view should start with the login page and it is shown below.



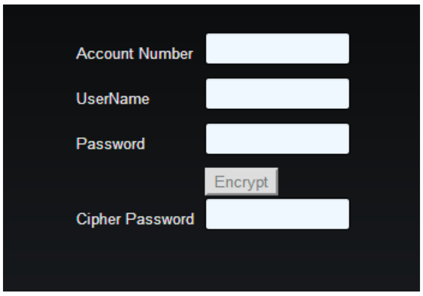


From Account No 20143852844

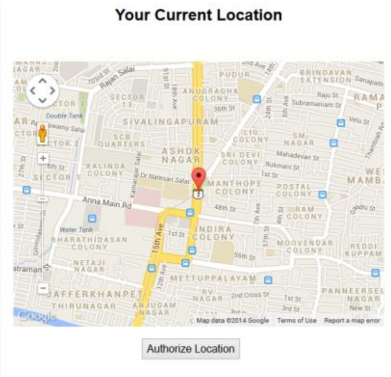
To Account No 2013918174259

Amount 3144

As far as the threat of the security injection is concerned, the counter measure can be a hashing technique. For such prevention the design for the following is shown below.

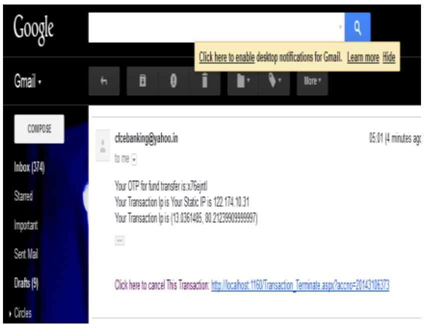


After the, access on the get my location, the page will be directed to the location tracing page. That will show the location of the user, that is the user's current location of the user.



After the authorization of the geographical location of the user, the location co-ordinates and the network IP details are sent to the users respective Email-ID with the additional OTP generated. This information is also passed to the user's Mobile device. The below mentioned snap shot is of the information sent to the Email-ID.

The main security signature of our proposed system is the generation of the cfc code internally and the geographical location tracing of the account user. The design of the location page tracing is shown in the below snap shots.



cfcebanking@yahoo.in
to me
05:01 (4 minutes ago)

Your OTP for fund transfer is:x76ejntl
Your Transaction Ip is Your Static IP is 122.174.10.31
Your Transaction Ip is (13.0361485, 80.21239909999997)

Click here to cancel This Transaction: http://localhost:1160/Transaction_Terminate.aspx?accno=20143106373

If the user is not the one using their own account and is the hacker or an intruder, then the original user can click on the link to cancel the transaction that will pass the message as transaction terminated.

7. CONCLUSION

Our aim in this study was to provide a full-fledged trusted, Nonobstructive secured system tailored for a cloud computing environment. To accomplish this task, we thoroughly reviewed the ways in which existing billing systems are used in the environment. We consequently derived blueprints for our proposed system. In addition to utilizing existing billing systems, we conceived and implemented the concepts of a CNA and S-Mon, which supervise billing transactions to make them more objective and acceptable to users and CSPs alike. Our proposed system features three remarkable achievements: First, we introduce a new concept of a CFC to ensure undeniable verification of any transaction between various network IP.Second,we trace the geographical location of the user to make aware to the users of their current location and of the intrusion if any.Third,we bind this both of the information and generate a OTP which is more efficient than any other OTP as it validates the location co-ordinates of the user..By integrating the module, we made the transactions more objective and acceptable in a more securable and in an efficient way to users and CSPs.

8. FUTURE ENHANCEMENT

In the proposed system the geographical location and network IP of the user is traced. Our next step is to consider the scalability and fault tolerance of system. The extension work in the future will be extending the capabilities of the trace back to be more accurate. The accuracy will be the exact location with the address of the location. We will also add on our feature with the IP address track. The users systems IP address can be tracked to add more securable feature.

In our work, The OTP and the link for the termination of the transaction is sent to the email and the user has to cancel the transaction by linking it through the mail.we will work for the link to be sent to the mobile device such that the user can terminate the transaction through mobile itself.

9. REFERENCES

1. .Amazon Web Services, "Amazon Elastic Compute Cloud EC2,Simple Storage Service," http://aws.amazon.com/ec2, http:/aws.amazon.com/s32, Apr. 2011.

2. Microsoft, "Microsoft, Windows Azure Platform," http://www.microsoft.com/windowsazure, 2010.
3. .Www.Researchinventy.ComSecure Login Using Encrypted One Time Password (Otp) and Mobile Based Login Methodology
4. .www.infosecisland.com/.../11813-One-Time-Passwords-are-Not-Secure

5. P. Vogt, F. Nentwich, N. Jovanovic, E. Kirda, C. Kruegel, and G. Vigna, "Cross-Site Scripting Prevention with Dynamic Data Tainting and Static Analysis", Proceedings of the Network and Distributed System.

6. A. Liu, Y. Yuan, A Stavrou, "SQLProb: A Proxybased Architecture towards Preventing SQL Injection Attacks", SAC March 8-12, 2009

7. D. Gollmann, "Securing Web Applications", Information Security Technical Report, vol. 13, issue. 1, 2008

8. Ter Louw, M; Venkatakrishnan, V. N.; "BluePrint: Robust Prevention of Cross-Site scripting attacks for existing

9. browsers", 30th IEEE Symposium on Security and Privacy, pp. 331-346, May, 2009.

10. Eric Ogren, "Whitelists SaaS modify traditional security, tackle flaws", Sep. 17, 2009. [Eric Ogren is the founder and principal security analyst at Ogren Group]

11. Gurdev Singh, Amit Sharma, Manpreet Singh Lehal, "Security Apprehensions in Different Regions of Cloud Captious Grounds", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011.

12. Zouheir Trabelsi, Hamza Rahmani, Kamel Kaouech, Mounir Frikha, "Malicious Sniffing System Detection Platform", Proceedings of the 2004 International Symposium on Applications and the Internet (SAINT'04), pp. 201-207, 2004

13. Jenni Susan Reuben, "A Survey on Virtual Machine Security", Seminar of Network Security, Helsinki University of Technology, 2007.

14. Flavio Lombardi, Roberto Di Pietro, "Secure Virtualization for Cloud Computing", Journal of Network and Computer Applications, vol. 34, issue 4, pp. 1113- 1122, July 2011, Academic Press Ltd. London, UK.

15. Hanqian Wu, Yi Ding, Winer, C., Li Yao, "Network Security for Virtual Machines in Cloud Computing", 5th Int'l Conference on Computer Sciences and Convergence Information Technology, pp. 18-21, Seoul, Nov. 30-Dec. 2, 2010

16. K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, "Intrusion detection techniques for Grid and Cloud Computing Environment", IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010.

17. Ruiping Lua and Kin Choong Yow, "Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network", IEEE Network, vol. 25, no. 4, pp. 28-33, July-August, 2011.