Advancement in GSM Network to Access Cloud Services

1Muhammad Tanveer Meeran, Asif Raza, Department of Computer Science, Bahauddin Zakariya University, Multan, Pakistan and Muizzud-Din, Department of Computer Science Khawaja Fareed University, RYK, Pakistan

Abstract- Cloud services are offering a large number of utilities to the mobile users. Mobile users can share, store, develop, compute and many other services on the cloud. Due to extensive utilization of cloud services by the mobile users, security concerns are also evolving with the same pace. Among different security problems, secure access to the cloud services (cloud data utilization, data storage) is also a difficult and challenging task. This paper highlights the security concerns, particularly addresses the issue of secure access to cloud infrastructure, such as access the cloud services securely by the mobile users. As Elastic Cloud Computing is valid only for Amazon, MLaden model is theoretical based model and not implemented practically, Wayne model enhances the end user security but not proposed tool for practical implementation. Intention of this paper is to propose mechanism to securely access the cloud services using GSM band. Only defined frequency band of GSM will provide the access to the cloud services. Users will be restricted to use the particular frequency to access the cloud services.

Keywords: Multi-Tenancy, Elasticity, Identity Spoofing, HLR, VLR and MSC.

I. INTRODUCTION

Cloud companies are offering different services. Such as: Saas (Software as a Service): This is consumer use app and don’t control/manange by network. It reduces expenses e.g. Flicker, Amazon, Cloud Drive. Paas (Platform as a Service): In this service cloud user or consumer deploy their apps on cloud computing system. But they can’t control, Manage, Storage Server. Iaas (Infrastructure as a Service): In this service consumer gets access of deployment of application, but don’t manage or control infrastructure. Instead of these it can manage and control storage and apps e.g. Elastic Cloud Complete (ECR).

Cloud computing concept is started in 1950’s with the mainframe computing. In which numbers of users or clients trying to access the mainframe through dumb terminals. But it is not feasible for each employee to install a mainframe [1]. After some time, nearly in 1970 the virtual machine concept generated [2] [3]. Through this different software used such as VMware software through this different operating system executed on the single physical hardware in different environment. Cloud computing helps the enterprises in different angle, it help the enterprises in reducing the
upfront cost of infrastructure deployment, helps the enterprises to focus only on their core business, helps in reducing the deployment time and costs, also provides the flexibility to the enterprises to meet their requirements on demand and enterprises only need to “pay as you go” basis.

Security concerns are increasing rapidly due to the extensive list of services for mobile user offered by cloud. Among different security problems, secure access to the cloud services is also a tough and noticeable task. By the analysis of previous models and techniques presented by researchers, their drawbacks are given in TABLE 1.

<table>
<thead>
<tr>
<th>Model/ Technique</th>
<th>Drawbacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC2 [4]</td>
<td>Is valid only for Amazon.</td>
</tr>
<tr>
<td>DS2 [5]</td>
<td>Provides end-to-end verification of data but their work is no longer valid.</td>
</tr>
<tr>
<td>TCPS [6]</td>
<td>Improved security, transparency mechanism but it is not deployed in professional cloud computing system.</td>
</tr>
<tr>
<td>Rongxing [7]</td>
<td>Presented mathematical model, system will be secured in all sense; but its implementation is difficult due to complex mathematical techniques.</td>
</tr>
<tr>
<td>MLaden [8]</td>
<td>It is theoretical based model and not implemented practically.</td>
</tr>
<tr>
<td>Provetrack.R.La [9]</td>
<td>Implemented a security capture device It is useful for end users or small systems; but it is not feasible for large scale companies.</td>
</tr>
</tbody>
</table>

By the viewing previous models or techniques and their drawbacks, proposed a new mechanism which is implemented by using the Paas (Platform as a Service) layer for secure access to cloud services over GSM network. By this approach previous shortcomings will be minimized.

The rest of this paper is organized as follows. In section II describes the security attributes and threats to the cloud services. In section III previous solutions of security will be discussed. Section IV elaborates the proposed solution for the cloud services. In section V results and analysis will be mentioned. Section VI pop out the conclusion in a best way.

II. SECURITY ATTRIBUTES AND THREATS TO THE CLOUD SERVICES

Basic security attributes are authentication, confidentiality, and integrity. Where authentication ensures that allowed person is accessing the data or only authorized person or devices can participate in communication within the network. Authentication is achieved either using digital signatures or certificates. Mostly RSA algorithm is used to ensure authentication [10].
Confidentiality ensures that data is confidential between intended parties and no one can see or read it without authentication of doing so. Different mechanisms and techniques are applied to the data to achieve the confidentiality [11].

Integrity ensures that data is original and real and data is not changed either during communication or in data storage. Different techniques [12] are applied to the data to maintain the integrity of data for examples hashes are generated for the data, which are the mathematical function. Hash functions not only ensure the integrity of data during communication but also during the store time over the data storage in cloud.

A. Threats to Cloud Services

In cloud computing data located at different places or locations. Because each server contains same type of data such as Mail server, File Server, Mom Server etc. The main purpose is to facilitate the user to access data from anywhere and anytime. But the scope of cloud is increasing constantly and security issues and risks are also increasing with respect to time [13].

List of threats to cloud services are given in TABLE II [14] [15] [16].

<table>
<thead>
<tr>
<th>Name of Threats</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tampering</td>
<td>An attacker may change the data which is stored in local file</td>
</tr>
<tr>
<td>Information disclosure / eavesdropping</td>
<td>In which attacker enter in the tunnel of traffic</td>
</tr>
<tr>
<td>Repudiation</td>
<td>Attacker tries to disprove the sender statement</td>
</tr>
<tr>
<td>Elevation of privileges</td>
<td>Attacker get access unauthorized to inform</td>
</tr>
<tr>
<td>Man in the middle attack</td>
<td>Attacker involve the third party deployment</td>
</tr>
<tr>
<td>Replay attack</td>
<td>After some delay of time data sent</td>
</tr>
<tr>
<td>Identity spoofing</td>
<td>Attacker destroy the identity of node or server</td>
</tr>
<tr>
<td>Viruses and worms</td>
<td>In which attacker slow down the performance of hardware and software as possible</td>
</tr>
<tr>
<td>Insider attacks</td>
<td>Low level of security due to illiterate staff working in cloud</td>
</tr>
<tr>
<td>Outsider attacks</td>
<td>Every hacker try to penetrate in API interfaces and break down the connection</td>
</tr>
<tr>
<td>Malware injection attacks</td>
<td>Attacker attacks in the form of any file type which is unknown for us</td>
</tr>
<tr>
<td>Flooding attacks</td>
<td>When system overloaded data not secured so, attacker access easily</td>
</tr>
<tr>
<td>Differential analysis threats</td>
<td>It occurred on the basis of old and new security codes</td>
</tr>
</tbody>
</table>
III. FORMAL SOLUTION OF THREATS AND ATTACKS

Table III below is showing formal solutions from the literature.

<table>
<thead>
<tr>
<th>Solutions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS2 [17]</td>
<td>Declarative secure distributed system (DS2) which provides end to end verification of data</td>
</tr>
<tr>
<td>EC2 [4]</td>
<td>EC2 Amazon and Python for Access security and Privacy in cloud computing. But drawback is that it is valid only for Amazon</td>
</tr>
<tr>
<td>TCPS [6]</td>
<td>TCPS) transparent Cloud Protection System. Presented model has improved security, transparency, and Intrusion detection mechanism. But their works not validated because it is not deployed in professional cloud computing system</td>
</tr>
<tr>
<td>Jinpeng [18]</td>
<td>Jinpeng (Jinpeng et al, 2009) they proposed an Image Management System model which provides Image filter, scanner to detect malicious images. But drawback is that image filter is not accurate sometime legitimate images may also be detected as malicious/ virus.</td>
</tr>
<tr>
<td>Mirandasiani [19]</td>
<td>Mirandasiani proposed a model in which many features were implemented like preference setting, data access and feedback but drawback is that it is not generalized and not implemented in all scenarios.</td>
</tr>
<tr>
<td>Rituik [20]</td>
<td>A simulation program is developed for eBay. It verifies billing detail and prevention of security attacks. But it is only applicable to sales application.</td>
</tr>
<tr>
<td>Dan and Anna [21]</td>
<td>Dan and Anna introduced a new framework with three key components, first is policy ranking, second is policy integration and finally policy enforcement. These components provide correctness, time efficiency, scalability, reliability and robustness. Drawback is that this model is not validated.</td>
</tr>
</tbody>
</table>

IV. PROPOSED SOLUTION FOR CLOUD SERVICES

This section provides the illustration of proposed work. A general scenario is presented below to depict the properties of proposed work. Scenario is based on the GSM architecture. Because overdue reports brought from the FCC [22] in the US and Ofcom [23] in the Uk have discovered the regular use within approved frequency bands is really as reduced as 5%. Due to availability of spectrum holes in GSM spectrum band, GSM network is involved in this approach. In this intention first section provides the brief overview of GSM architecture and second section provides the details of integration of proposed work with the GSM scenario. General GSM architecture can be shown in Figure 1.

Figure 1: General GSM Architecture
Figure 1 illustrates the general influence of signals through GSM architecture. Where, as per requirement cloud services can be accessed and managed by the server. In this architecture accessed services and data flow will be less secure due to less security implementation. Other reason of the less secure of GSM network as GSM is public network so any one can utilize this network. The encryption methods, hashing techniques [24] may secure the network but hackers also have the ability to decrypt these methods as well. The pictorial view of mentioned scenario is given in Figure 2.

![GSM Network in Detail Working](image)

Figure 2: GSM Network in Detail Working

Figure 2 illustrate the detail mechanism of the GSM architecture. This architecture describes the complete detail of each part of the GSM network. First part describes the registers which are using in GSM. There are two types of registers that are commonly used. (i) Home Location Register (HLR) saved the permanent address of the subscribers. (ii) Visitor Location Register (VLR) saved the temporary data of the visitors. Figure2 shows that Mobile Station (MS) directly linked with Base transceiver Station (BTS) and BTS connected with Base Station Centre (BSC) and BSC with Mobile Switching Centre (MSC) and MSC send or receive the data or services through clouds or any public or private networks or via internet.
Figure 3: GSM Network and Proposed Scenario

Figure 3 shows the communication between MS and cloud. According to this secure access method adopted by implementing the digital filter which is software defined radio (SDR) module which can filtered out the particular frequency from a GSM band spectrum. This particular frequency used only for a specific purpose. This frequency utilized only for cloud services (data storage, data integration, and data analytics). Software defined radio module (Digital filter) communicate between MS and GSM. MS and BTS communicate by using the Um interface and BTS communicate with BSC via Abis interface. Same as above mentioned BSC communicate with MSC through an interface

Digital filter (SDR) is connected with BTS terminal. When MS want to communicate with cloud or want to access cloud services then it use the particular frequency which can be extracts from GSM band spectrum by using the digital filter (SDR). MS has the mobile equipment (ME) and subscriber identity module (SIM). MS send the request to the GSM spectrum for attaining the specific filtered frequency; BTS send the acknowledgement to the MS and send the message to the SDR to filter out the required frequency. After receiving the message SDR starts to perform its functionality and acknowledges the BTS. After that, BTS send the acknowledgement to the MS and MS tune the application according to the required frequency, so through this method secure cloud services accessed between MS and cloud.

GSM have the different parts which can communicate with each other. Cloud services which we want to access, these services may be data storage, data integrity and data analytics. Secure access method might be possible by using these different devices but for implementing the proper statistical and mathematical equations we can justify and explain the proposed work. For the justification and explanation of this model we should equate the proper equations, which are in the form of general
equation and in the form of statistic. Now, the general and static form of given model is given below.

\[ \text{GSM} = f(\text{MS, CLOUDS}) \] 
\[ \text{(1)} \]

In the equation 1 GSM is the main variable which is the functionality of MS and clouds. MS and clouds depends on GSM because if GSM not exist/implemented then communication between MS and GSM is not possible. Basically these are all the variables which is dependent on GSM and GSM is independent variable. On the other hand MS and clouds are dependent variables. If we separately discuss these dependent and independent variables, then these variables have the different communicating parts, such as the dependent variables MS have the ME and SIM. Clouds have the junk of data and have a many more parts but our concern is only related to data storage, data integrity and data analytics. Independent variable is GSM which have the BTS, BSC, MSC, HLR, VLR, AUC, EIR etc.

Second form of equation which we are elaborate in this model is Statistic form of equation that is

\[ \text{GSM} = \alpha_0 + \alpha_1(\text{MS}) + \alpha_2(\text{CLOUDS}) + \mu_o \] 
\[ \text{(2)} \]

The equation 2 shows the statistical form of the cloud scenario/model. \( \alpha_0 \) shows the intercept and \( \alpha_1 \) shows or denoted the slope of the given variables.

\[ \text{GSM} = f(\text{BTS, BSC, MSC, HLR, …………N}) \] 
\[ \text{(3)} \]

In this Eq. 3 GSM is a dependent variable which has been used in this model that represents BTS, BSC, MSC, HLR, VLR, AUC, EIR, OMC and others. Specifically GSM is interrelated with all this functions such as BTS, BSC, and MSC and so on.

\[ \text{MS} = f(\text{S, M}) \] 
\[ \text{(4)} \]

MS is interconnected with the mobile Sims and mobile equipment. Cloud includes storage, integrity and analytics. It means that

\[ \text{CLOUDS} = f(\text{data storage, data, integrity, data analysis}) \] 
\[ \text{(5)} \]

V. RESULTS AND ANALYSIS OF PROPOSED WORK SIMULATION

For accessing cloud services using GSM Network concept of SDR as digital filter is designed. To access services, a signal of particular frequency in licensed band of GSM is generated. For this purpose a licensed band created. After that, define signal will propagate in defined frequency ranges with other undefined signals. In last our digital filter extract out defined signal. The detail of this
entire scenario, i.e. defined signal frequency, licensed GSM band, multiple signal propagation, extraction of defined signal is depicted step by step with all requirements.

A. **Signal Generating and Conceptualization**

In Figure 4 contiguous blue lines describe the defined signal using mathematical equation \( \cos(2\pi t \cdot \text{frequency}/20) \) for time period 1 sec at frequency 1000Hz. Basically it is the generation of defined signal for accessing cloud services.

![Figure 4: Defined Signal](image)

B. **Spectrum Generating and Conceptualization**

After defined signal generation next step goes to Spectrum generation. On the basis of scenario, Spectrum is generated with sampling frequency 1000 Hz and having frequency range 0 to 1000 Hz, is shown in Figure 5.

![Figure 5: Spectrum Generation](image)
C. Multiple Signals Broadcasting in Same Spectrum

As spectrum holes are there in GSM band, to enhance the efficiency of spectrum, a number of users utilized band. So in the same spectrum band defined signal broadcast with other signals. This phenomenon is shown in Figure 6.

![Figure 6: Multiple Signals Broadcasting](image)

D. Extracting Defined Signal through SDR (Digital Filter) from GSM Band Spectrum

When defined signal broadcast in defined GSM band then defined signal modified due to addition of noise. Where blue spark lines in Figure 7 show this. Whereas black dotted lines shows the undefined signal. After removing the noise from defined signal to carry out cloud services, blue dotted lines in Figure 7 obtained after the filtration of defined signal from noise.

![Figure 7: Extracting Defined Signal](image)

D. Analysis on Defined Signal

Analysis is performed on defined signal. Analysis of signal is performed in term of spectral power density, Autocorrelation.
i. Power Spectral Density

Power spectral density is a very valuable tool. Power spectral density exposes the intensity of frequencies variations and at whatever variations are feeble by utilizing the strength of the alterations (energy) as a function of frequency. PSD integrating within frequency range, energy within that specific frequency range is gained. Inspection of variation in frequency domain is reliable way to noticing time series data variations and frequency transformation of time. PSD demonstrates which frequency dimensions alteration are intense and for further analysis that would be quite useful. Table 4 demonstrate the PSD of defined signal that is extracted from GSM band spectrum. PSD calculated at different frequencies are listed in Table 4.

<table>
<thead>
<tr>
<th>Frequency (Hz)</th>
<th>Power (dB)</th>
<th>Power MilliWatts</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>-18.83</td>
<td>13.0918</td>
</tr>
<tr>
<td>20</td>
<td>-44.61</td>
<td>.03459</td>
</tr>
<tr>
<td>40</td>
<td>-52.14</td>
<td>.006109</td>
</tr>
<tr>
<td>60</td>
<td>-61.7</td>
<td>.000676</td>
</tr>
<tr>
<td>80</td>
<td>-59.75</td>
<td>.001059</td>
</tr>
<tr>
<td>100</td>
<td>-58.98</td>
<td>.001265</td>
</tr>
</tbody>
</table>

In similar way Table 5 demonstrate the PSD of original defined signal before propagation.

<table>
<thead>
<tr>
<th>Frequency (Hz)</th>
<th>Power (dB)</th>
<th>Power MilliWatts</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>-18.81</td>
<td>13.1522</td>
</tr>
<tr>
<td>20</td>
<td>-44.61</td>
<td>.03459</td>
</tr>
<tr>
<td>40</td>
<td>-52.14</td>
<td>.006109</td>
</tr>
<tr>
<td>60</td>
<td>-61.9</td>
<td>0.000645</td>
</tr>
<tr>
<td>80</td>
<td>-59.75</td>
<td>.001059</td>
</tr>
<tr>
<td>100</td>
<td>-58.96</td>
<td>.001270</td>
</tr>
</tbody>
</table>
Both extracted defined signal PSD and original signal PSD graphical representation can be view in figure 8 which depict that defined signal that is propagating in licensed GSM band after implementation of proposed technique PSD of it remain same without interfering other signals.

\[ \rho = -1 \]
\[ \rho = 0 \]
\[ \rho = +1 \]

**Figure 8:** Comparative Analysis of Power Spectral Density

### ii. Auto Correlation

Correlation is a relationship that exists between signals. Correlation procedures are broadly utilized as a part in signal processing with numerous applications in media communications, material science, stargazing, geophysics and many more.

Numerous valuable properties of correlation has been given, for example the ability to
- Perceive designs within analogue, discrete-time or digital signals.
- Correlation is an examination procedure
- The correlation between two functions is a measure of their comparability.

When measuring the correlation between two functions, the result is often expressed as a correlation coefficient, \( \rho \), within the range \(-1\) to \(+1\).

\[ \rho = -1 \]
\[ \rho = 0 \]
\[ \rho = +1 \]

<table>
<thead>
<tr>
<th>Similar but opposite</th>
<th>No similarity</th>
<th>Exactly similar</th>
</tr>
</thead>
</table>

For periodic functions, with period \( T \), the correlation function is given by [25]

\[ R_{12}(\tau) = \frac{1}{T} \int_{-T/2}^{T/2} v_1(t) v_2(t - \tau) \, dt \]  

\[ \text{--------- (6)} \]
R12(τ) is the correlation function and is a measure of the similarity between the functions v1(t) and v2(t). The measure of correlation is a function of a new variable, τ, which represents a time delay or time shift between the two functions. That correlation is decided by multiplying one signal, v1 (t), by someone else shifted in time, v2 (t-τ), and finding the integral of the product, in this fashion correlation concerns multiplication, time shifting (or delay) and integration.

Autocorrelation, identified as serial correlation. In signal, the perception of autocorrelation has meaningful aspect of tragedy. Autocorrelation action of signal suggests the generic dependence of codes of samples at one time on codes of sample at other time. Informally, it is similarity between considerations as a function of the time lag between them. The ACF (Autocorrelation function), R(τ), is noticed as by [25]

\[ R(\tau) = \frac{1}{T} \int_{-T/2}^{T/2} v(t)v(t-\tau)dt \]  

------------- (7)

For auto correlation, the correlation coefficient is given by [25]

\[ \rho = \frac{R(\tau)}{\sqrt{R(0).R(0)}} = \frac{R(\tau)}{R(0)} \]  

------------- (8)

Resultant correlation coefficient of original signal and filtered signal are computed in MATLAB, which are given below

\[ \rho = \begin{bmatrix} 1.000 & 0.8732 \\ 0.8732 & 1.000 \end{bmatrix} \]

As all calculated correlation coefficients are close to 1, as a result there is a strong positive correlation between each one pair of data which depict that signal extracted from licensed band is similar to original signal. No one can access the cloud services without knowing the frequency of defined signal. If anyone get to know the frequency of defined signal successfully, then digital filter is programmable which can alter the frequency of defined signal simultaneously. Further encryption techniques enhance the security. So by this eaves dropping, outsider attack and malware injection are minimized.

VI. CONCLUSION AND FUTURE DIRECTIONS

Proposed developed scenario will be helpful in providing the secure access to the cloud services (cloud data utilization, data storage). Secure access to the cloud services provided by implementing
the signal of defined frequency in licensed GSM band which is generated by using software defined
filter. Only defined frequency range will provide the access to the cloud services. Users are restricted
to use the particular frequency range to access the cloud services. In this way security threats to
cloud computing can be minimized and access to the cloud services can be restricted.

More research is required to develop New and modern techniques to remove vulnerabilities found
in licensed bands for quick and efficient access to cloud services.

REFERENCES

Engineering.


2010, Chicago, USA.


Switzerland.

[7] Rongxing et al, —Secure Provenance: The Essential Bread and Butter of Data Forensics in Cloud Computingl,
ASIACCS’10, Beijing, China


[13] Issa M. Khalil et al, security concern in cloud computing,2013 10th international conference on information

technology: New Generation.


Chauhan

[16] A Survey on Cloud Security Issues and Techniques Garima Gupta1, P.R.Laxmi2 and Shubhanjali Sharma


Computing.

Pittsburgh, Pennsylvania, USA.


/emerg tech / cograd / cograd_main.pdf


Signals in Small Cutaneous Vessels”.IEEE transactions on ultrasonics, ferroelectrics, and frequency control, vol. 47,
no. 6, november 2000