Internet Penetration in African Countries and the Road Map to Strengthen Ethiopia for its IT Challenges with IT Structure and Guidelines Available in India

Dr. Garima Sinha[1], Dr. Deepak K. Sinha[2]
[1]*Assistant Professor, Department of Information Sciences, Wolkite University, Ethiopia*
[2]*Assistant Professor, Department of Computing, Jimma University, Ethiopia*

Abstract - The internet is penetrating the Ethiopia at the rate of 1.90% or more and the current scenario is, less than 1% population is using internet here. The world is focusing on African countries for their business for the IT enabled services and the Mobile based services, as today world is growing rapidly with the help and support of these services and here there is a great scope to incorporate these features. In Ethiopia, like everywhere else, progress can be measured with IT, Mobile and technologies in use at different service sectors in the country. In addition to that, technology has its downsides: malware, threats and cyber-crime, due to the huge scope of internet proliferation and penetration in different services and sectors, the scope of cyber threat and crime is also possible here. We are trying to keep a look on the all possibilities to strengthen Ethiopia for its current and future IT challenges with IT structure and guidelines available in India. This paper is an attempt to study about all current possible weakness available in the infrastructure of the mobile and IT networks at Ethiopia and how it can be defined and solved with the help of network and IT Infrastructure of India. This paper will also focus with the law and regulation of the cyber crimes of both the countries for betterment and strengthening the future IT and mobile technologies challenges of the country.

Keywords: Cyber Treat, Mobile Treat, Internet Penetration.

I. INTRODUCTION

The world greatest Economist were forecasted that the world's top six fasted growing countries are in sub-Sahara African countries. There rapid booming sectors are infrastructures and IT services like Mobile Technology and the web based services. As per the reports, the top 50 countries with reference to the economy will be potential countries from African reasons. The African Development Bank are also expecting that there will be a makeable increase in the per capita income of the people across the African countries and consumer paying capacity by within next 15 years, Resulting many MNC's are trying to get a chance to develop IT market in this continent and many of them had already arrived here with great hope and doing their business in this region.

The world is focusing on these African countries for their business for the IT enabled services and the Mobile based services, as today world is growing rapidly with the help and support of these services and here there is a great scope to incorporate these features.

We must not forget here that every coin has two phases a head and a tail, and hence, the incorporation of the technology also may lead to this region in different directions, we are already known to the positive aspect of the technology implementation in different services across the globe, where it is already in use. Now our study is focused on the side effects of the IT and Mobile based services, which is being used by the banking systems in Ethiopia. We have restricted our study on the possible cyber threats and mobile frauds in Ethiopia and there remedial measures available as per the technology available in India.

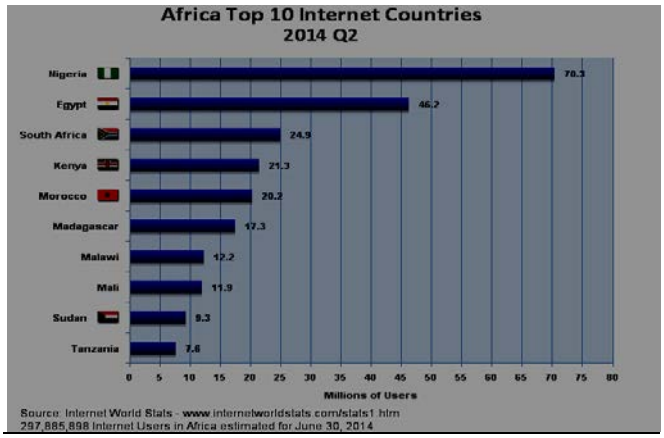
In Ethiopia, like everywhere else across globe, progress can be measured with IT, Mobile and technologies in use in the services at different sector in the country (we are only focusing on the banking sectors). In addition to that, technology has its downsides: malware, threats and cyber-crime.

II. SECURITY ISSUE

The Ethiopia is one of the high potential country, which may go for Internet penetration in coming days, and it is expected to rise the number of internet user exponentially, well this is a good news and a bad news also, as the increase in the number of IT user may lead to the a problem of the cyber

threats, crimes, hacking and many more in near future, and hence, it is a matter of great concern also for the services sectors especially. For this paper we have taken the E-Banking related cyber threats in Ethiopia.

III. STUDY OF THE TRENDS OF THE IT USERS IN AFRICAN REGIONS AND IN ETHIOPIA



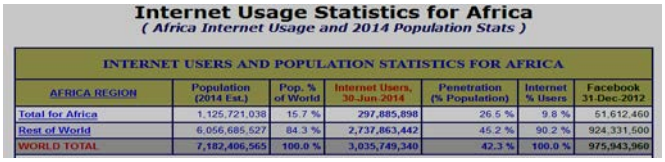
Source: http://www.internetworldstats.com/stats1.htm

Sl. No.	AFRICA	Population (2014 Est.)	Internet Users 31-Dec-00	Internet Users 31-Dec-13	Penetration (% Population)	Internet % Africa	Facebook 31-Dec-12
	AFRICA 2014 POPULATION AND INTERNET USERS STATISTICS FOR 2013 Q4						
1	Nigeria	177,155,754	200,000	**67,319,186**	38.00%	28.00%	6,630,200
2	Egypt	86,895,099	450,000	**43,065,211**	49.60%	17.90%	12,173,540
3	South Africa	48,375,645	2,400,000	**23,655,690**	48.90%	9.90%	6,269,600
4	Kenya	45,010,056	200,000	**21,273,738**	47.30%	8.90%	2,045,900
5	Morocco	32,987,206	100,000	**18,472,835**	56.00%	7.70%	5,091,760
6	Sudan	35,482,233	30,000	**8,054,467**	22.70%	3.40%	n/a
7	Tanzania	49,639,138	115,000	**6,949,479**	14.00%	2.90%	705,460
8	Algeria	38,813,722	50,000	**6,404,264**	16.50%	2.70%	4,111,320
9	Uganda	35,918,915	40,000	**5,818,864**	16.20%	2.40%	562,240
10	Tunisia	10,937,521	100,000	**4,790,634**	43.80%	2.00%	3,328,300
11	Ghana	25,758,108	30,000	**4,378,878**	17.00%	1.80%	1,630,420
12	Angola	19,088,106	30,000	**3,645,828**	19.10%	1.50%	645,460
13	Senegal	13,635,927	40,000	**2,849,909**	20.90%	1.20%	675,820
14	Zimbabwe	13,771,721	50,000	**2,547,768**	18.50%	1.10%	n/a
15	Zambia	14,638,505	20,000	**2,254,329**	15.40%	0.90%	327,600
16	Ethiopia	96,633,458	10,000	**1,836,035**	1.90%	0.80%	902,440

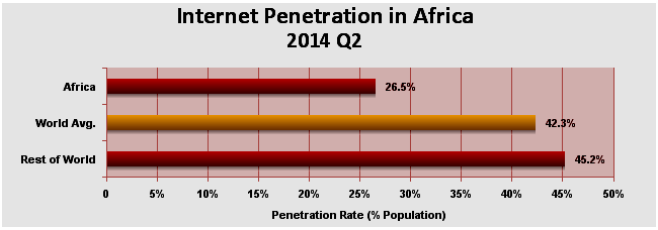
Source: http://www.internetworldstats.com/stats1.htm
(Figure-1)

The Ethiopia is not in the top 10 countries, which is having maximum internet users at Africa, now the question is the Ethiopia is lying at which position; the data below is the analysis of all countries across the Africa with their Internet penetration with respect to the population and number of Internet users.

The above figure(Figure-1), showing the result of some African countries in their descending order of their internet penetration and the internet user, there are about 57 countries in the Africa and the Ethiopia is at number 16, based on the number of Internet User and the penetration rate of the Internet user at Ethiopia.



Source: http://www.internetworldstats.com/stats1.htm
(Figure-2)



Source: http://www.internetworldstats.com/stats1.htm
(Figure-3)

Figure-2 and Figure-3 shows that the average percentage of the internet users and penetration percentage at Africa and across the globe. We can see the remarkable differences, the average of Africa is at the level of the Internet user is 9.80% and the penetration percentage in Africa is 26.5%, where as rest of the world percentage of the Internet users are 90.20%, almost more than 10 times of the African users and the penetration percentage is 42.30%, which is almost two times of the penetration percentage of the Africa.

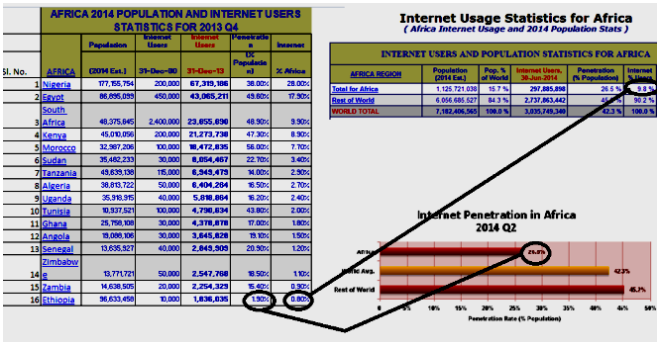


Figure-4

Figure 4, shows the competition of the internet users and penetration percentage of the Africa with reference to the Ethiopia, we can see the remarkable difference between the two, the internet users percentage in Africa is 9.8% where as

at Ethiopia is 0.80, which is almost 1/12 of the rest of the African users. And if we compare the Internet penetration percentage, at the Africa, it is 26.50% as compare to the Ethiopia, which is having only 1.90%, which is 1/13 of the African Internet Penetration percentage.

The most interesting thing is if we look at the world internet penetration average it is 45.2%, but if we see it the average excluding Africa it is 42.3%, which is 2.9% less than the world average, it means that the Africa is only contributing 2.9% internet penetration to the whole world.

IV. E-BANKING SERVICES IN ETHIOPIA

The good thing is the Internet User percentage and the Penetration percentage is growing at the same speed in Ethiopia with respect to the population, and the other very good news is that there is great scope for the IT and Mobile based services to be launched here at every service area again there is a great chance for the fraudulent activity too using these services.

Following services are being offered now days in Ethiopia under E-Banking:

V. INTERNET BANKING

Through Internet banking, many transactions can be carried out from the comfort of your home or office. The online services include:

- Viewing account balances and transactions.
- Making fund transfers between customers's own current accounts and savings accounts.
- Effecting payments to third parties, including bill payments to predefined customers within Ethiopia.
- Presentation and downloading current and saving account statements.
- Requesting for discontinue payments on cheques, etc.
- Applying for a letter of credit…and more…

Using Internet banking facility, customers will benefit from our personal and Corporate Internet Banking services that are available, 24 hours a day, 7 days a week, from any location.

Source www.combanketh.et , www.cbeib.com.et

Limitations and the threats using Internet banking:

As per the unofficial records, very few customers are using Internet banking here in Ethiopia, due to the following reasons:

- The less number of Internet users in the country.
- Less penetration percentage in the country.
- Lack of awareness program towards the Internet banking.
- Lack of mobile version site of CBE.
- Lack of Internet infrastructure to the remote areas, and
- The most important is to use Internet banking one has to register his/her device.

The biggest drawback among the above is the point number 6, that is, if you wish to use Internet banking and its related facilities then first of all you are supposed to register the device to which you are accessing the Internet, which leads to the restriction of the uses from the Internet banking either form the home or form the office, which is a great limitation in our view.

- A customer may not have a personal Internet device.
- The device may be cloned and there may be a chance of fraudulent activities.
- His/her office may not permit him/her for the financial transactions.
- The office may not give him the details of the Internet connection for the personal use.
- The office may put some, DLP devices and his confidential data may lose in the public network of the office LAN.
- If you lost your device, you will have to do the entire activity of Internet banking once again.
- The same Internet device may not work to the other countries and hence a customer may not be in a position to use Internet banking, exterior the country.
- Cost of Internet is very tall in Ethiopia.

5.1 ATM

ATM has introduced in Ethiopia by CBE, With ATM card, you can bank 24 hours a day and 7 days a week.

Enjoy a host of services, including

- Cash withdrawals

- Bill payments
- Forex
- Fund transfer
- Mobile top up
- Balance inquiry, etc.

5.2 MOBILE BANKING

Mobile Banking services enable you to:

- Access your bank accounts,
- Make fund transfers,
- costs and balance inquiries as well as
- Get instant notifications

On all your accounts associated with MB services-using the SMS, XHTML and DOWNLOADABLE application channels".

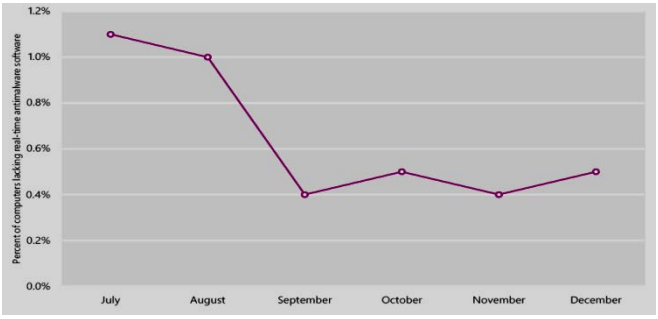
Mobile Banking and the ATM services are almost on the same platform as compare to the other countries and banking systems, the banks here got membership of the VISA/MasterCard card and the ATM services are same as compared to the other continent banking systems.

VI. THREAT AND CONCERN TO THE INTERNET BANKING

There are many threats and concern to the E-Banking system, but we are only concerned here with the possible cyber threats in and around the country (Ethiopia). The possible threats for the E-Banking across the world are:

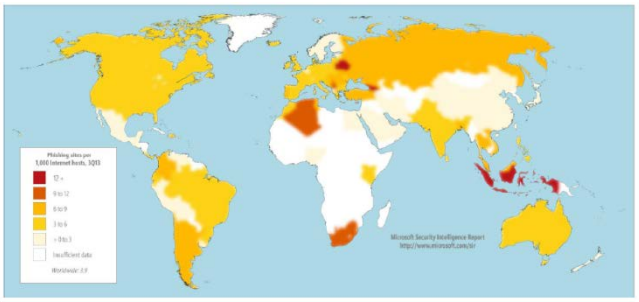
- Phishing
- Unauthorized use of Internet banking
- Unauthorized use of Mobile banking
- Unauthorized use of ATM banking
- Fund Transfer using cyber frauds, etc.
- Fraud mails regarding sharing of the personal data.
- Win Lottery mails.
- Account details on phone.
- Card Skimming
- Fake Websites
- Fake Jobs
- Password Sharing.

Now we want to analyze how safe we are, as per the Microsoft Security Intelligence Report 2013, the number and percentage of the system running with real time antimalware software are decreasing day by day, if we look at the study of last 6 months in the year 2013, it dropped from 1.1% to the 0.5% across the globe and undoubtly the case must be same for Ethiopia.

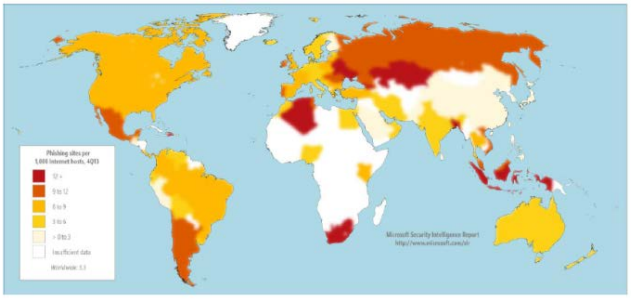


Percentage of computers at Microsoft not running real-time antimalware software in second half 2013.

Now the major concern about the E-banking is phishing, and the hackers are using this tool to steal our valuable data with the help of phishing as one of its hacking tools.



Phishing sites per 1,000 Internet hosts for locations around the world in 3rd Quarter 2013



Phishing sites per 1,000 Internet hosts for locations around the world in 4th Quarter 2013

The phishing tools and sites are increasing day by day across the globe and it may affected the E-banking and Internet banking across the globe and the CBE should take a note on it and must give a awareness program for their valuable clients/customers. If we took a look at the graph of the phishing sites it has significantly increased during 3rd

quarter (July-September) to the 4th quarter (October-December) 2013.

Country/Region	1Q12	2Q12	3Q12	4Q12
Ethiopia	9.7	10.5	9.1	11.3
Worldwide	***6.6***	***7.0***	***5.3***	***6.0***

Computer Infection Rate at Ethiopia in the year-2012, all four quarter(Source-MSIR, Vol-14, 2013)

As per the sources (MSIR, Vol-14, 2013) the infection rate of the computer in Ethiopia has raised from 9.7% to 11.3% within a year, whereas the worldwide infection rate has dropped from 6.6% to 6.0% within a year and really it is a serious concern for the Internet users and the Internet based E-banking applications in Ethiopia.

Country/Region	Encounter rate 3Q13	Encounter rate 4Q13	CCM 3Q13	CCM 4Q13
Ethiopia	—	—	24.8	28.9
Worldwide	*20.21%*	*21.58%*	*5.6*	*17.8*

Ethipian Encounter and Infection Rate (Source-MSIR-Vol-6, 2014)

If we consider the date (Source-MSIR-Vol-6, 2014), the encounter rate between quarter three 2013 was 20.21% and it raised to 21.58% in the next quarter (4th quarter) 2013 the data of the encounter rate is not known for the Ethiopia, but the CCM at Ethiopia was increased from 24.8 to 28.9 form 3rd quarter 2013 to 4th quarter 2013, which is significantly high as compare to the worldwide average CCM form 3rd quarter 2013 and 4th quarter 2013, which was 5.6 and 17.8 respectively.

VII. Remedial Measures that should be taken in as per the Guidelines Available in India for E-Banking

The following guidelines are available by the RBI in India for the safe and secure E-Banking in India, which is recommended here for any possible or future threats in electronic financial transitions in Ethiopia. The guidelines are as follows:

Technology and Security Standards

The bank must have clear cut guidelines for the technology as well as the security standards, the bank must assign a network as well as the database administrator and he/she should be given a clear-cut policy and guideline to follow it strictly.

The banking system to implement the E-Banking, the bank should use the logical access and also grant the permissions to their clients by this logical access like, user-ids, passwords, cards(debit/credits), biometric devices etc.

The bank should have a proxy server, so that the direct connection can be avoided between the bank and the internet connections.

The SSL (Secured Socket Layer), which can be used for server authentication and client side certificate issued by the bank, must be implemented, and use of at least 128 bit SSL for the communication between the browser and the web server, and the encryption of the sensitive data like passwords etc.

The bank should have sufficient infrastructure for the back-up of the data and it must be periodically tested.

All the banking transactions should be double secured by two types of passwords like, user passwords and the transactions passwords and to make it more authentic the E-banking must be integrated with the mobile of the customers and the bank must generate OTP during transactions at the registered mobile numbers.

VIII. Study of the Trends of the Mobile Users in African Regions and in Ethiopia

Mobile Penetration in Ethiopia

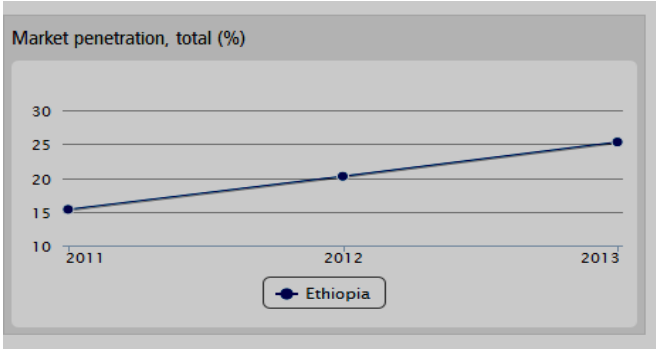
As per the records of GSMA Intelligence Survey for 2011-2013, Ethiopia is eleventh country in the Africa in terms of number of mobile users, it is now expected that there are more than twenty five millions mobile subscribers are available in Ethiopia now a days.

Sl. No.	Region	Country	2011	2012	2013
1	Africa	Nigeria	94908699	112408197	126880410
2	Africa	Egypt	84926206	96605104	99601080
3	Africa	South Africa	57703574	65382673	70433736
4	Africa	Morocco	36554000	39016230	42439617
5	Africa	Algeria	35615926	36393536	39517045
6	Africa	Kenya	28080771	30731754	31309017
7	Africa	Congo, Democra	16491792	22110672	30277315
8	Africa	Ghana	20752828	25055031	27679937
9	Africa	Sudan	24193763	27478000	27624844
10	Africa	Tanzania	23457682	26888405	27160635
11	Africa	Ethiopia	13893095	18805000	24108406
12	Africa	Mali	10819784	14604653	19744308
13	Africa	Uganda	16336522	17486146	19467938

Total of mobile connections registered by mobile operators in a country.

This is also one of the parameter to measure the growth and development of a country on the basis of the adaptation of Mobile and its related technology and its use in a country.

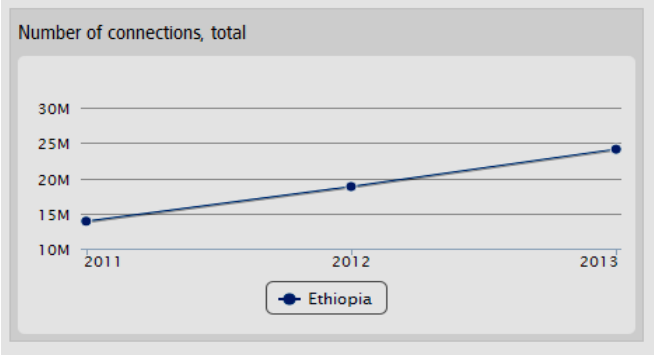
Range: 2011 – 2013, Source: GSMA Inetelligence



Total of mobile connections registered by mobile operators in a country.

Mobile is penetrating in the market of the Ethiopia at the constant rate of 5% per annum, so the current market penetration is in between 24 to 29% and the subscribers are lying somewhere in between 24 to 29 millions in Ethiopia.

Range: 2011 – 2013, Source: GSMA Intelligence



Total of mobile connections registered by mobile operators in a country.

Range: 2011 – 2013, Source: GSMA Intelligence

The only mobile service provider in Ethiopia is Ethio telecom, which is having following mobile based services:

- Mobile Services
- Internet Services
- Fixed Land Line Services
- Business Set up Solutions (VSAT etc)

As per a report there may be more mobile devices on the earth than the people and the average age to use mobile is now gone down to 13 years, but still approximately 25-29% population is only using the mobile services and it is increasing at the rate of 4-5% per annum, so there is a great scope of the penetration and proliferation of this services here in Ethioipia, as we know that we make technology for the convenience of the mankind but it is used for the fraudulent activities also. The threat areas where this can be applied in Ethiopia are:

- Cloning of SIM
- Duplication of IMEI number
- Fraudulent Calls

We will discuss about the Fraudulent Calls first, as in Ethiopia, the pre-activated SIM Cards are available, you are simply suppose to give the copy of the ID and you will be given pre-activated SIM and you can enjoy the Mobile services without wasting a seconds, As per the procedure, the ID verification and submission to the corporate office will take approx three months time. This is a great threat in the mobile technology here.

The second threat is cloning of SIM and cloning of IMEI number of the mobile handset, if the cloning of SIM is done then the all Credit/Debit cards transaction is possible and it is a matter of great concern across the globe. The remedial measure to check the SIM cloning is to use only genuine and authentic mobile handsets with valid IMEI numbers, IMEI numbers are the numbers given by GSMA and it is a 15 to 17 digit unique number to every mobile handset. IMEI numbers either come in a 15 or 17 digit sequence of numbers. These numbers can identify a handset.

Currently, the IMEI's format is AA-BBBBBB-CCCCCC-D.

These two digits (AA) are for the Reporting Body Identifier, indicating the GSMA approved group that allocated the TAC (Type Allocation Code).

BBBBBB – The Remainder of the TAC

CCCCCC – Serial Sequence of the Model

D-Luhn Verify Digit of the entire model or 0 (This is an algorithm that validates the ID number)

The service provider can check the validity of the IMEI (International Mobile Equipment Identification Number) by

incorporating the Luhn Algorithm to their existing software, which can work as follows:

The last number of the IMEI is a ensure digit. The verify Digit is considered according to Luhn formula.

The Check Digit is a function of all other digits in the IMEI. The idea of the ensure Digit is to help protector against the possibility of incorrect entries to the CEIR and EIR equipment.

The CEIR (Central Equipment Identity Register) is a central IMEI database service that updates different local EIR's from all operators in one system. The basic functionality of this CEIR is to maintain a white, grey and black list of all IMEI numbers by all connected operators.

The check digit is validated in three steps:

1. Starting from the right, double a digit every two digits
2. Sum the digits check if the sum is divisible by 10.
3. Conversely, one can calculate the IMEI by choosing the check digit that would give a sum divisible by 10.

For example: IMEI: 91123305065916-3

(1x2, 2x2, 3x2, 5x2, 6x2, 9x2, 6x2) = (10, 8, 2, 0, 8, 2, 2)
(2+4+6+1+0+1+2+1+8+1+2) + (9+1+3+0+0+5+1) = 47
Luhn Digit: 3

IMEI: 911233-05-065916-3

IX. Guideline available for the possible Mobile Threats in India

9.1 Mobile device with only valid IMEI can be registered on the mobile network by the mobile service providers.

9.2 No pre-activated mobile connection can be distributed, a customer may take a SIM card or mobile connection after submitting the valid ID, but it will only work after verification of the ID and verification of the personal details on the first activation call by the service provider/telecom authority.

9.3 Now, the TRAI is going to introduce a regulation regarding the lost/missing mobiles, that there IMEI numbers should be blocked, so that they may not be registered on any of the network further and it cannot be duplicated to any other handset with invalid IMEI numbers.

What to do if your phone is theft or lost?

9.4 First of all the case should be reported to your mobile operator and to local police station. After this you can put forward your phones IMEI number to global stolen phones database. Numerous people checks the database and can recognize your mobile before buying it from second hand (if it is submitted in database

9.5 It is possible in India to check the validity of the IMEI number by sending IMEI to number 53232 or 57886; a client will get a message without any delay about the authenticity of the IMEI number. We may also promote the same thing here to strengthen the possibility to detect invalid or duplicate IMEI of the Handsets in Ethio telecom network.

X. Conclusion

There is a huge scope and potential of internet penetration and applications related to the internet in Ethiopia, it is penetrating at the rate of 1.90% in the population with the increase in the rate of Internet users, the risk of cyber crimes/fraud are likely to be increased with more rate than the Internet penetration rate in the population. The law for the cyber crime/fraud is either lying at very infant stage or not properly implemented; in that case the Ethiopia can be a heaven for the cybercriminals or may be a safe place for the cyber related crimes and criminals, the same is the case with the Mobile threads also, as it is expected to grow exponentially in near future and the rate of mobile related crimes is also expected to grow here in near future.

References

[1] D. K. Sinha, G. Sinha, E-Banking in Ethiopia and the consequences due to increase in the cyber threats/Crime across the globe: Trends and Concerns, IJETCAS, Vol.4, Issue 10, September-November 2014, ISSN(Print)-2279-0047, ISSN(Online)-2279-0055

[2] IDG Connect, Cyber Crime Hacking and Malware, Africa 2013

[3] Meseret Lakew, Computer Related Crimes in Ethiopia (Comparative Study), 2008 www.abyssinialaw.com.

[4] Bhaskar Reddy and Twedros Sisay, E-Business :Application of Software and Technology in Selected Ethiopian Banks: Issue and Challenges., IJCSI, Vol 8, Issue 6, No 1,Nov. 2011. www.ijcsi.org

[5] Oluminde Longe et. all, Criminal Uses of Information and Communication Technologies in Sub-Saharan Africa: Trends Concerns and Perspectives, Journal of Information Technology Impact, Vol. 9, No.-3, pages 155-172, 2009

[6] The National Information and Communication Technology Policy and Strategy, Addis Ababa, 2009

[7] Eric Tamarkin, Policy Brief, The Institute of Security Studies, www.issafrica.org.

[8] Gardachew Worku, Electronics-Banking in Ethiopia-Practices, Opportunities and Challenges, Journal of Internet Banking and Commerce, Vol. 15, No. 2, August 2010.

[9] MSIR, Vol.-14, July Through December, 2012

[10] MSIR, Vol-16, World Wide Threat Assessment, July through December,2013

[11] www.combanketh.et , www.cbeib.com.et

[12] http://rbidocs.rbi.org.in/rdocs/notification/PDFs/21569.pdf

[13] Jenny C. Aker and Isaac M. Mbiti, Mobile Phones and Economic Development in Africa, Journal of Economic Perspectives—Volume 24, Number 3—Summer 2010—Pages 207–232

[14] http://www.abyssinialaw.com/uploads/761.pdf

[15] http://www.ethiotelecom.et/