Vol 7. No. 3 - September, 2014
African Journal of Computing & ICT

www.ajocict.net

A Social Engineering Detection Model for the Mobile Smartphone Clients

A.A. Ojugo
Dept. of Mathematics/Computer
Federal University of Petroleum Resources
Effurun, Nigeria
ojugo.arnold@fupre.edu.ng

A.O. Eboka
Department of Computer Education
Federal College of Education (Technical)
Asaba, Delta State, Nigeria
andre_y2k@yahoo.com

ABSTRACT

The continued advances in both Internet and mobile smartphones has up-scaled client adoption of Internet-based data processing activities like e-banking etc. These, have also necessitated growth cum deployment of mobile applications across platforms to help clients accomplish data processing tasks by harnessing its many benefits. Yet, it has also exposed clients whom are today, constantly besieged by data security threats that are not limited to social engineering attacks. Thus, towards data residence, sensitive and proprietary – clients have become bothered with the exposure of their smartphones to possible data loss, theft, manipulation and inspection etc – if they are to further adopt these new paradigms. These, leaves fears and doubt in the mind of clients (as data owner) and reduces their trust-level in such services. We propose a client-trusted security model for smartphones employed in banks that aims to increase clients' trust-level in the adoption of mobile banking – making it more dependable as the framework seeks to address security threats with transaction authenticity and message authorization. Results shows framework is capable of increasing client's trust level in relation to social engineering attacks with about 72% as implemented over their firewall by the banks (for Internet connectivity as well as ported on a community-cloud) for user access.

Keywords—phishing, whaling, framework, social engineering, financial institutions, fraud, vishing, smishing

African Journal of Computing & ICT Reference Format:
A.A. Ojugo & A.O. Eboka (2014). A Social Engineering Detection Model for the Mobile Smartphone Clients.
Afr J. of Comp & ICTs. Vol 7, No. 3. Pp 91-100.

1. INTRODUCTION

SIgnificant advancement with the field of information and communication technology (ICTs) has since climaxed with exponential growth and advancements of the Internet that continues to beam its benefits to its plethora of clients or users. These can today, be seen to have permeated into the fabrics of our daily lives and activities, as we employ ICTs for personal, business and recreational purposes. ICT continues to advance efficient dissemination of data for effective decision making. A corresponding sine-qua-non effect is the myriad of threats that seeks to exploit the inherent vulnerabilities in these advances of ICT and associated technologies for many of its naïve users. These challenges and threats manifests in various forms or ways presenting itself as misleading items of benefits to many 'unsuspecting' users, and aimed at defrauding them [1]. ***Fraud*** is a criminal act, perpetrated via embezzlement, larceny and theft in which a criminal employs falsehood to benefit from an unsuspecting patron, or from assuring victim of great returns (if it is aimed at a financial transaction) such that the victim relies on such falsehood.

A transaction is exchange of goods and services for gains or money deliverables [2]. Criminals find it easier to exploit users of a service than exploiting a web application or network connection, and many organizations who invest in highly sophisticated security often fail to adequately address their biggest vulnerability, which is deception of their employees. However, criminals increasingly use deceptive means to exploit corporate business practices and circumvent controls so as to trick unsuspecting clients into sending money or diverting payments to imposters [2][3].

Social engineering (not a new paradigm) has steadily grown with no-end-in-sight. Its continued growth borders on human nature of trust instincts, on which hackers manipulate human emotion and ultimately, exploit this trust to steal valuable information. Common technique for achieving this feat are: phishing, vishing, smishing etc – with the most popular being phishing.

It uses social engineering and technical subterfuge to defraud an online account holder of their financial information by posing as a trusted identity. Phishing can be executed via multiple means including: spoofed emails and phone calls, web link manipulation and forgeries, man-in-the-middle chat, covert redirect etc – all aimed at convincing a user to divulge confidential data and/or participate unknowingly in fraudulent transactions [4].

These attacks are mostly targeted at clients that employ Internet daily, from which a greater multitude continues to adopt the mobile smartphone. These attacks have thus risen in number for smartphone clients – resulting from the increased growth of user access to mobile smartphones from 42.5% in 2013 to 78.9% by 2013 and the advent of Androids is made smartphones a preferred choice over personal computers due to its design, portability, speed, functionality and ease of Internet access. All these, continually pose significant threats with its high vulnerability rate and security risk to user data. Consequently, these have its range of implication to work-related functions and business issues as it often exposes sensitive data to adversaries. Even with advancement cloud computing to the rescue, data security challenges still persists with many impediments into the full realization of its potentials and benefits as it seeks to explore storage capability to guarantee data recovery of user data at various levels [2].

Data and applications shared both on the ***Internet*** and as extended via ***cloud*** computing – really resides in systems that the clients have limited or no control over. And though, in both instance, transaction or message authentication is done by client – there are often no checks or measures that allows for authenticity feedbacks or handshaking is performed between the client and service provide, to confirm from each other the validity of a transaction or message. This has become a major challenge, and today, is quite responsible for most security issues associated with both cases of the Internet and as extended via cloud technologies. Other security concerns for service providers include: (a) possible harm to an organization for public distributed access, (b) recovery cost implication from such harm, and (c) other associated risks that may result in service failure or denial of service. These concerns (should) raise questions in the minds of its many prospective clients – since the inability to resolves these challenges, leaves them bewildered and insecure towards adopting these services, irrespective of its many benefits even in the foreseeable future [2][4].

Thus, the ***idea*** or objective of this study is to develop and deploy a framework model for early detection of fraudulent activities spawning from or geared towards social engineering attacks that are aimed at smartphones clients.

A. Social Engineering

A client (or end-user) of a service can perform a transaction by send a message to another user or executes control message as sent to such a client by the service provider. Thus, client is given access to a plethora of services by the service provider. With social engineering attacks, many see the obvious victim as the client engaged in using the service; But, actual target of the attack is the service provider or organization. For financial services companies (banks), many of her services to clients can be potentially damaged with social engineering schemes like phishing. In 2015 alone, over 67% of phishing attacks were trading on names of banks and financial organizations, while 61% of the phishing attempts were specifically targeted at the financial credentials. Phishing exploits are becoming more successful and even now, exceedingly more difficult to detect (as most of them go unreported). 23% of above fact were lured to open phishing messages; while, 11% were lured to open its attachments [5]. These attacks may be aimed at the unsuspecting user on the obvious; But, the actual claim is that it continually undermines the client's and/or user's confidence in a brand, puts the client at great risk of identity theft (to mention few) and consequently, incurs huge financial losses, debts and deficits to the financial sector or industry. As phishing and other social engineering attacks escalate, financial institutions are soon enmeshed in recruiting new means to track and mitigate these attacks and its potential damages; While, they constantly battle to remain updated in both the finance and ICT world [2].

B. The Android Smartphone Framework / Platforms

Smartphones are today, a preferred device of choice over the personal computers for some data processing activities due to its ease of Internet access, portability, durability and speed of processing (with its seemingly user-satisfaction of upload and download time, and to mention a few). Many of these employ various operating systems that allow it to perform many of the much user-needed feats of data communication and processing activities. Examples of such operating systems today include: Android, Windows, Symbian, iOS, Blackberry etc.

[6] Android is today, a leading platform for mobile devices owing from its open source feat to distinguish it from other platforms such as Blackberry, Windows Phone and iOS. It is not a specification nor distribution of traditional Linux, neither is it a collection of replaceable components or chunk of software ported on a device. Its open source platform is built by Google with OS, middleware, and applications for mobile platforms based on Linux kernel – enabling developers to write apps majorly in Java with support for C/C++. A major success is in its licensed under Apache2, allowing third party porting-developments to the platform. Since its release, it has been constantly improved either in feats, supported hardware, and at same time extended to new device types from the originally intended mobile ones [7]. Recent efforts are geared towards enhancing for real-time capabilities, to be employed in variety of other embedded systems [6][8].

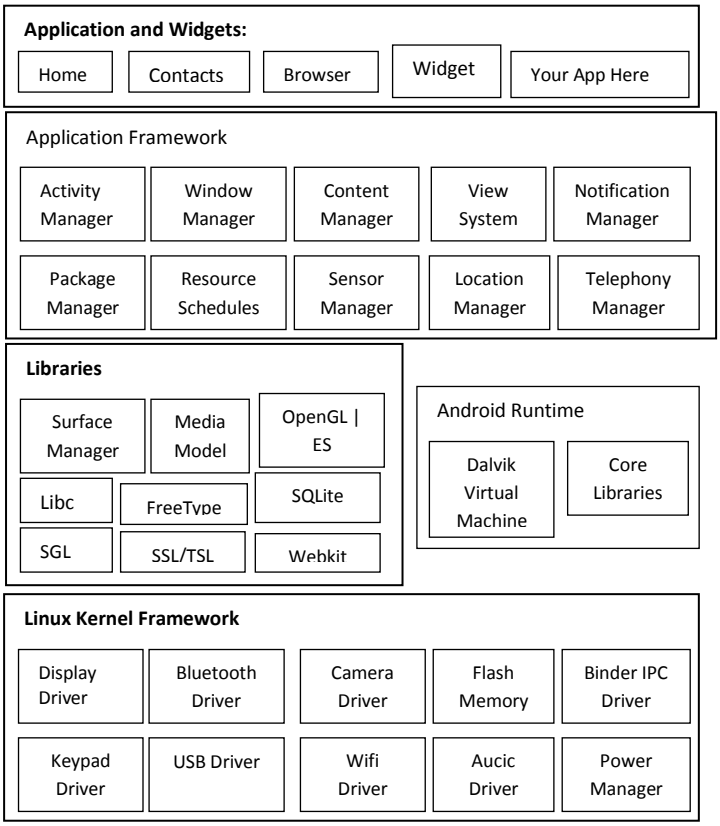

Fig 1: Android OS Platform

[9][10] in "Google Android and Linaro Android SDK" note that the Android Platform is an eco-system layer of software component implemented on the mobile smartphone hardware as thus (see fig 1) and at whose core are these features:

a. Linux OS provides basic functionality such as security, process/memory management and networking to support vast device drivers. It handles human machine interfaces, file systems, network access etc. Its kernel is modified by Google to use low memory killer, specific inter-process communication system, kernel log feats, shared memory system and many other changes as developed. It runs on standard Vanilla Linux, merging specific changes into its kernel. Recent release aimed at real-time Linux kernel is v4.0.3 (Ice Cream Sandwich).

b. Library with Google's *libc* called *Bionic*, media/graphics (OpenGL|ES), browser-webkit and light-database SQLite. DVM (Dalvik Virtual Machine) completely differs from Sun's JVM and uses register based byte code to conserves memory, max performance and can instantiate many of its apps multiple times, with each app having its own private copy running. DVM uses Linux for memory management and multi-threading to support the Java language.

DVM uses *bionic* (not compatible with *glibc*) so that its native libraries are faster to implement with small custom *pthread* to support services such as system and logging capabilities. Writable data segments are small so as to be loaded into memory with each process. This keeps code size small so that Linux loads only once, all read-only pages. *Bionic* is used: (a) to avoid inclusion of GPL code at user space level in its platform where BSD is used, and (b) for small memory footprint devices with high speed CPUs at relatively low frequencies. *Bionic libc* does not handle C++ exceptions (though omitting such lower level exceptions pose no problem as Java is Android's primary language. It handles exceptions internally). *Bionic* has no priority inheritance for mutexex as implemented in *glibc*. Available in its kernel and accessed via own library in system calls, its lack of priority inversion disqualifies it for real-time capability as applied in robotics/automotive. Google's reason for a complete new VM from scratch as accomplished with DVM's register-based byte code is to reduce patent infringement risk. Thus, existing real-time apps modified for JVM cannot easily be ported to DVM.

c. Application Framework provides higher-level services to apps such as Java classes amongst others. Its use can vary between/with varying implementation.
d. Application/Widget are Android routine distributed apps such as email, SMS, calendar, contacts and Web browser.

C. Security Concerns and Controls

Many of the security concerns and risks associated with both the Internet and extended by cloud technologies can be safely handled by organizations via planned risk management in biz processes and activities. Examples of these include: (a) the right to choice of service provider, (b) the legal responsibility that must be accepted by service provided, the threat of access to intellectual properties, and (c) content of disaster recovery documentation [11-12]. But, lack of control on the physical infrastructure is responsible for most of the security issues that arise in both instances of the Internet and cloud. Furthermore, clients are ignorant of the physical location of their stored data in the distributed environ as well as what security mechanisms are in place to guard their data and defend them against hackers and other adversaries [13].

Also, security issues relate to web services and web browsers for mobile smartphone clients on the Android platform, is addressed in [6]. These can be adapted to other platform technologies as the most common attacks on web services is XML Signature Element Wrapping with XML signature used in authentication of a transaction or message [12].

Security controls are required in all ICT-enabled environ. In addition, the Internet presents different risks to different client as they access it due to the services requested for, operations to be performed as well as technologies of smartphone devices that are associated with it. Internet security control models can be applied: (a) to applications via firewalls, (b) to data via database activity monitoring, (c) managing infrastructure via configuration management and monitoring, (d) to intranets and other forms of network via firewalls, and (e) data storage via encryption schemes. Use of traditional security controls like access controls and encryption, monitoring of large internal data migrations with database/file activity monitoring, and monitoring of data movements via the Internet with URL filters and data loss prevention [6].

2. MATERIALS AND METHODS

Dataset Used

Available social engineering data is as in Table 1 and table 2 – represented as in Fig. 1 and fig. 2 respectively.

Table 1: Target List of Social Engineering represented in Fig 1

No	Types of Organisations	Percentage
1	Social Sites	15.2
2	Financial and Banking Services	34.4
3	Portals	19.7
4	Military	9.8
5	Government Officials & Top Management Personnel in Government Parastatals	8.3
6	Others	12.6

Table 2: Kaspersky Target List of Phishing Attempts

No	Phishing Attempts On	Percentage
1	Financial Credentials	21
2	Recipients Opening Phishing Messages	23
3	Recipients Opening Phishing Attachments	11
4	Vishing, Smishing, Whalling and Others	45

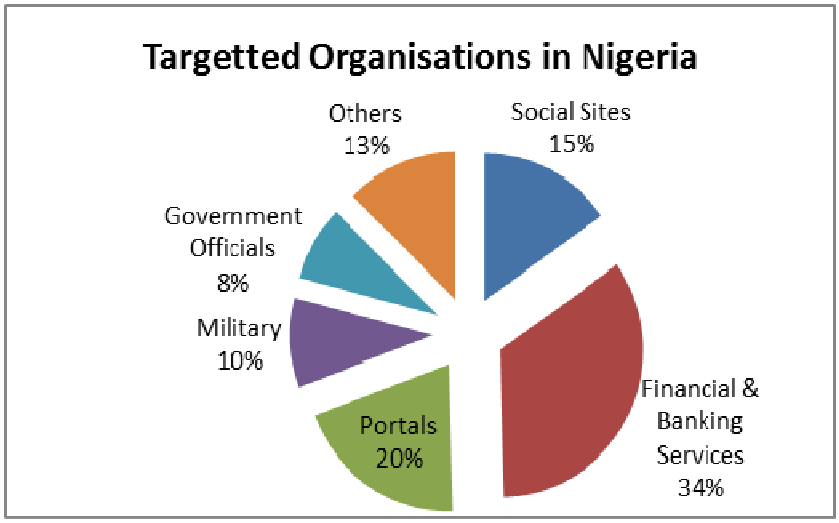

Fig. 1: List of targeted organs by Social Engineering Attacks

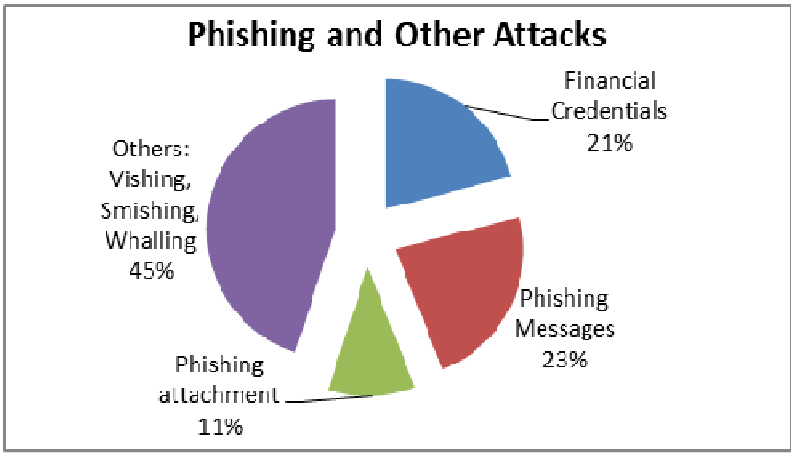

Fig. 2: Phishing Attacks and Others

The ***study*** seeks to model authentication and authorization framework for smartphone clients in financial transaction. This will aid clients to evade and avoid socially-engineered attacks and fraud aimed at smartphones.

D. Statement of Problem

The problem statements are as follows:

1. Advancement in Data Security continually beckons on the exchange of data to update awareness of techniques used by hackers as well as exchange of data in fraud detection, which is often limited as it is unwise to describe in public domain (fraud detection techniques in great detail). As a dual effect, it will further equip organisations, users and hackers with adequate information required to combat as well as evade significant detection (for hackers). Thus, we employ statistical fraud detection method and heuristics as in Section III.
2. A major challenge clients face in accessing the Internet, is that of message authenticity – as it is difficult for a user to differentiate between a service provider's message (as is case of 'targeted' financial institution's websites) and a fraudulent one, leaving them exposed to fraud and attacks.
3. Unavailability of social engineering (fraudulent) datasets due to unreported cases as well as its ***uncensored*** results, and the non-establishment of regulatory organs to monitor such activities, makes fraud detection, its techniques and consequent studies, difficult to assess. Also, the available dataset are plagued by noise, ambiguities and impartial truth. These, must be resolved

via accurate classification models and algorithms that seeks to efficiently classify observations and expected values of rules generated from the dataset. This is resolved in Section III/IV.

4. Another major challenge is that the banks have no control on authorization decisions as a hacker can easily convince a client to generate a signature and authorize a fraudulent transaction without the bank's involvement. This is because in a typical process, the bank has zero control over the authorization decision – even with the use of *Digipasses* (hardware mini tokens). The client completely authorizes any of his banking requests at any given time – including fraudulent ones. This is a major reason why phishing continues to be successful.

The goal and objective of the study is to provide a framework that achieves the following:

a. In using a mobile banking platform – the client is required to configure the device used and synchronize data with the banking 'mobile-device' database, which registers and authenticates a client's banking details with the mobile device used. This aims to remove the issue of trust and trust decision, out of the hands of the client and ensuring that when a client request is made to initiate a transaction, the bank in tandem with the client initiates and grants access to a transaction signature request. This can be achieved using a cryptogram.
b. The bank establishes a secure communication channel between the client's device and their platform that enables the message and transaction to be authenticated.
c. Ensure that the bank controls the authentication process as the client initiates any and all transactions.

3. PROPOSED EXPERIMENTAL MODEL

Client data stored in smartphones have become easy targets for malicious attempts. Clients may not understand security features as provided in varying forms, needed to be in place as they constantly access Internet and other computing platforms. Thus, study proposes a reliable modeled framework that seeks to help users uncover and detect socially engineered attacks that are aimed at smartphones.

The framework seeks to bring a sense of control to many of the Service providers (infrastructure and services) as well as grant a failsafe to mobile smartphone via a single platform via mobile computing. It is an extension of the miniaturization process and faster computing on Moore's law, bringing about dependable and secure data storage capability to users via portable mobile devices.

The framework is designed to thwart efforts geared towards social engineering attacks via phishing, vishing, smishing and whaling (to mention a few). It is now customary that very often, most clients use ***digipass*** (or ***tokens***) to authenticate their every mobile banking transactions or messages (between them and their banking institutions) from their trusted device (smartphone) via either the hardware or software form for message and transaction authentication as well as client authorization. As thus:

a. Cryptogram – [6] GSM and CDM/FDM are grouped under second-generation systems. *GSMs* are developed to resolve incompatibilities in the cellular technologies so that a number of subscriber units can be used. Its basic feats are: subscriber Identity Module (SIM) portable smartcard-like plug-in device that stores a user's identification number, the network a client is authorized to use, encryption keys, and other info specific to a user or subscriber. Terminals are generic until SIM is inserted so that the subscriber unit and SIM roams; Transmissions between base transceiver and user is encrypted with ***A5*** cipher; while, ***A3*** cipher helps authenticate calls making it private to a user. GSMs support data and image services based on ISDN (Integrated Service Digital Network) model with user data rates upto 9.6kbps.

   The advent of third-generation communication system allowed mobile subscribers and personal communication services to incorporate set of standards and services unto the mobile unit (making them smartphones) so that it can then support data in form of voice, files, image and video. Though, housed within the device is the cipher (A5 and A3) that helps to authenticate data sent between devices and the service provider. However, banks can provision for extra layer of cryptogram that allows further ciphering so that the data packets (messages or transaction) initiated by a client as sent via a client-trusted device encoded for adequate authentication by the bank. The cryptogram contains all transaction data, including: registered device in use, transaction amount, and recipient account details.
b. Digipass (Hard/Soft tokens) addresses clients' transaction authorization and message authentication weakness via and by assuring the bank that only a registered/authorized client can authorize a legitimate transaction, so long the bank is able to verify the user details which includes (not limited to): registered device in use, account details and benefactors (recipient from another bank) etc [14-16].
c. Data Configurable Model allows for trusted computing via virtualization. Virtualization simply is the process of decoupling hardware from an OS on a physical machine. The Internet (and Financial institutions today), via mobile banking provide users with multiple isolated environ or sites, known as virtual machines (VMs) on a single host. VM is a virtualized representation of a physical machine that runs or is maintained on a host machine by software virtual machine monitor (hypervisor), to provide trusted computing, a mechanism that allows financial institutions to verify their security posture through hardware/software controls. A key component is the trusted platform module (TPM), which is a cryptographic component that provides a root of trust for building such a trusted computing base. Its goal is to move cryptographic computations into a locked virtual area, which is not under control of entities on the host platform. TPM works only in non-virtualized environs. A virtual Trusted Platform Module is provided according to standard specs by creating an instance of TPM for each VM on a trusted

platform. All these layers of security – helps to act as measures to ward-off hackers and intruders [17-20].

d. Web Services API – Framework seeks to implement an AES-256 encryption, which is easily ported and supported by SSL/TSL. We adopt this for: (a) it is computationally secure against brute-force, (b) flexible, (c) small-size Java codes allows support for C-language, (d) memory size required is small as ported on Android platform as it has no effect on the performance of memory and speed of the smartphone, and (e) ease of integration as implemented with Java and support for C-language into its web browsers with ease of connectivity. Also, the Chrome and Firefox Web-browsers can be used as they all allow AES-256 encryption. Since, data transfer over the Internet between a client and his/her service provider remains unprotected, no matter how good SSL in use is.

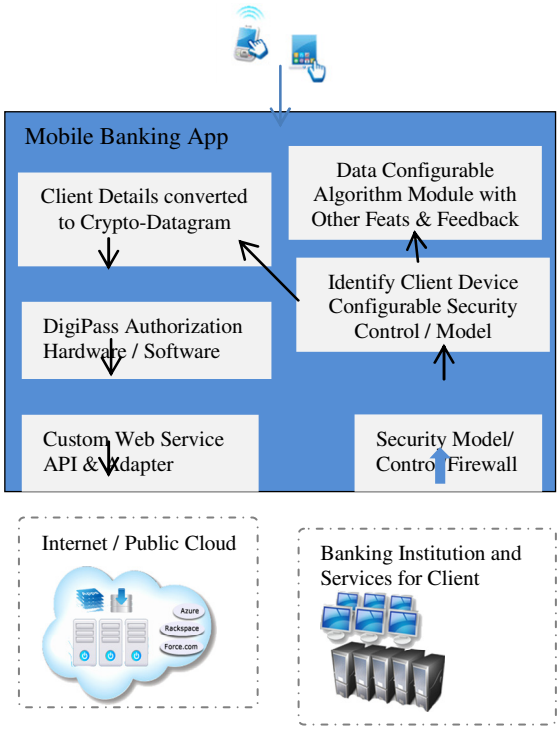

Fig 4: Application and Data Model For Smartphone

The study provides a framework security model for clients using smartphones, and operable on the Android v2.4 platform with support for web-service to allow easy access to Internet connectivity and connection to remote server/cloud-services via API call (adapter). Framework masks all technical nuances between application-model and data-models such as session management, connectivity-issues, transaction authentication and message authorization between a client and his/her bank. Its security is first handled via the digipass that generates a user personal identification number (PIN) from the hardware device (called a token). It is worthy to note that the device is already registered to the user so that whatever token generated can allow the user to log unto his account via the A5 and A3 ciphers provided natively by the mobile smartphone device [21-24]. Furthermore, the client's smartphone device is then used to log unto the bank's platform bypassing their firewall – having been granted access via generated token so that sent message are authenticated and initiated transaction are verified by the bank to originate from an authorized client. The system then uses the cryptogram to ensure that transactions and messages are properly formatted according to the bank so that they are allowed to efficiently be transmitted via the AES-256 crypto-system on SSL/TSL as applied to all data. Its client end-to-end encryption solution uses AES-256 to protect its data; while SSL protects username and password (see fig. 1).

Tools used for the development of this native app include Android SDK, Apache XAMPP and Google's Android Studio. This native app is enabled and ported on any Android platform from v2.2 with forward compatibility.

E. Experimental Implementation and Findings

The proposed framework was tested through comparison and evaluation with live and running scenario of a community-cloud provider (as well as connected over the Internet) and a user. The user is natively connected to the Internet via his/her smartphone device, and also subscribed for IaaS services via

FUPRE community-cloud to US-based cloud service provider for purpose of installing some proprietary mobile smartphone applications. Product details for the cloud provider, options available and values set are as in Table 3; while, the provider's level of Client Trusted Process Model of proposed model requires documentation (as in Table 4).

Table 3: Smartphone Internet Provider's Product Options

Product Details	**Options set**
Registration Date:	5/27/2012
Product/Service:	Online Traders - VPS Value Edition
CNS Subscription ID:	118223
VM:	VM118223.tradersvps.net
IPv4 Address:	173.228.134.65
Number of Snapshots:	1
CPU Cores:	2
RAM (MB):	640
DISK (GB):	20
Two-factor Authentication:	No
VNC:	Do not install VNC
Operating System OS:	Traders VPS Windows 2003 (x86) Enterprise Edition R2
Language:	English
Datacenter:	NYC
Payment Method:	MasterCard, Visa & Am- Express
First Payment Amount:	$30.00 USD
Recurring Amount:	$30.00 USD
Next Due Date:	8/27/2016
Billing Cycle:	Monthly
Status:	Active

The location of the datacenter, the description of the Virtual Machine, monthly rate paid by the user, the security control provided by the provider and other product information are shown in Table 1. It is seen from Table 1 that the only security control provided by provider is "Two-factor Authentication".

Table 2: Security Control with Documentation Proposed Connectivity

Security Control Name	Documentation Label and Documentation
Two-factor Authentication	**D1**: As a client initiates a log in from registered smartphone device unto the bank's platform, it requests that the client be verified at each log-in request. Thus, the bank verifies if the client is an authorized user via the token generated by the digipass and authentication message. Also, each client is prompted to re-verify at each log in session and/or having successfully logged off from the banking platform. The user can also request a token be sent to him/her for verification via SMS if such a user does not have a the hardware token (though this would not be the usual case). This currently exists for most cloud platforms
Use secure provisioning and Secure Migration Protocols	**D2**: These protocols prevent data from ever being sent to malicious hypervisor, virtual machines and host whenever a new virtual server is requested on the cloud. It puts a verification mechanism in place to ensure that that attacks against the virtual environment of your stored application or data will not be performed by an unapproved Operating System.
Virtual Trusted Platform Modules	**D3**: Virtual TPM protects its internal data from being accessed by the host environment, hypervisor, and all other virtual environments on the platform and puts a protection in place to prevent itself from being cloned and it is maintained in a secure location under your full physical control.

Security control with documentation for proposed framework using simulation is shown in Table 4. Proposed framework uses 3-security control systems at point of data configurable algorithms. The user trust level increases with the number of operational and well document security controls. Comparing the initial values with Table 4, the proposed framework is capable of increasing the trust level of the client by about 72 % when compared to the existing cloud system.

The users trust can increase above this value as more appropriate security controls are put in place to clear the user's doubt and enhance the trust level.

F. Benefits Accrued to Client and Institutions

Some benefits to be provided by the framework include :

a. Help combat social engineering and other online banking threats
b. Mitigate human risk in online banking transactions
c. Works with push notifications to immediately alert a client when updates and other information are made available by the service provider
d. Enables flexible deployment on any screen as the client can work between his trusted device and computer system – and vice versa.
e. Improves user experience of mobile (smartphone) online banking via its scan and sign that enables fast adoption and brings both safety and simplicity to user when signing transactions.

G. Related Study

[6] uses integrated framework for dependable community-cloud computing for smartphones. Study provides a support tool ***PushCloud*** that allows clients access a user account with the capability to sign-in and perform backup functions on contacts, messages, picture files, documents, videos and recorded voice amongst others via their smartphone unto the cloud with access granted via their service provider. The system proffers benefits such as the ability to pool together cloud service providers, provides a user with a cross-platform with minimal price difference as well as aim to address security-related issue from a user's end via AES-256 encryption on the integrated cloud model. This it does while exploring storage capability to guarantee recovery of data from a remote server (BDC) for back-end as well as front-end data storage ease [25-28].

4. CONCLUSION AND RECOMMENDATIONS

In this study, we model a client smartphone framework for detecting and warding off social engineering attacks and fraud. The model is designed to help address and thwart social engineering attacks by taking the 'trust' decisions out-of-the hands of the client, ensuring that while only a client initiates a transaction, authentication and authorization is domiciled with the bank to verify that the said transaction is by an authorized client via his trusted device (smartphone) [29-31]. Although deception fraud attacks will likely continue with increased frequency and sophistication, most organisations will equip themselves with the capability to minimize and mitigate all risks they and their (prospective) clients will encounter. While, the good news is that it does not require a massive ICT budget; It does however require more of commitment on the part of the financial institutions (banks) to invest time and resources into employee education and training (as possible threads for threats is most likely to come from them as they are better disposed to the flaws inherent in their system) as well as invest into their system to safeguard their future with their clients. As a result, there is no excuse not to implement basic deception and/or fraud security measures, and every company (financial organisations) should consider insurance as an important component of their overall risk management program[32-35].

REFERENCES

[1] Yeboah-Boateng, E.O and Amanor, P.M., *Phishing, smishing and vishing: an assessment of threats against Mobile Devices*, Journal of Emerging Trends in Computing and Information Sciences, 2014, Vol. 5, No. 4, pp297-307

[2] Ojugo, A.A., D. Allenotor., D.A. Oyemade., O.B. Longe., C.N. Anujeonye., *Comparative study for credit-card fraud detection models*, African Journal of Computing and ICT, 2015, Vol. 8, No. 1, Issue 2, 2015, Pp 15 - 24

[3] Symantec Corporation, *Internet Security Threat Report*, 2015, Vol 20, www.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-reportvolume-20-2015-social_v2.pdf

[4] Alnajim, A.M. *Fighting internet fraud: anti-phishing effectiveness for phishing websites detection*, unpublished doctoral dissertation, 2009, Durham University, Durham

[5] VASCO Data Security: *Social engineering vulnerabilities Report*, 2015, Vol 12, www.vascodata.com/mktginfo/whitepaper/ISTR/internet-security-threat-reportvolume-20-2015-social_engineering_phishing..pdf

[6] Ojugo, A.A., Aghware, F.O., Yoro, R.E., Yerokun, M.O., Eboka, A.O and Anujeonye, C.N., *Dependable Community-Cloud Framework for Smartphones*, American Journal of Networks and Communications. 2015, Vol. 4, No. 4, pp. 95-103. doi: 10.11648/j.ajnc.20150404.13

[7] Maia, C., Nogueira, L and Pinho, L.M., (2010). Evaluating Android OS for Embedded Real-Time Systems, Proceedings of 6th International Workshop on Operating Systems Platforms for Embedded Real-Time Applications, Brussels, Belgium.

[8] Tapas Kumar, K and Kolin, P., (2010). Android on Mobile Devices: An Energy Perspective, IEEE 10th International Conference on Computer and Information Technology, Kuala-Lumpur, Malaysia.

[9] Pernel, L, Fayyad-Kazan, H and Timmerman, M., (2013). Android and real time application: take care, J. Emerging Trends in Computing and Info. Systems, 4, Special Issue ICCSII, ISSN 2079-8407.

[10] Agam, S., (2011). Google's Android 4.0 ported to x86 processors, retrieved online via: http://www.computerworld.com/s/article/9222323/Google_s_Android_4.0_ported_to_x86_processors.

[11] ISACA White Paper, *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*, 2009, p1-10 [online]: www.klcconsulting.net/security_resources/cloud/Cloud_Computing_Security_&_Governance-ISACA.pdf Accessed July 2016.

[12] Babu, G. N. K. S., Srivatsa, S. K., "Security And Privacy Issues in Cloud Computing", International Journal of Engineering, Business and Enterprise Applications, 2014, pp 145-149.

[13] Jensen, M., Schwenk, J., Gruschka, N and Iacono, L. "On Technical Issues in Cloud Computing". In IEEE International Conference, Honolulu: Piscataway, 2009.

[14] Banday, M.T., Qadri, J.A. *.Phishing - A Growing Threat to E-Commerce,* The Business Review, 2007, ISSN: 0972-8384, Vol. 12, No. 2, pp. 76-83.

[15] Bankash, A., *For detailed information on PWSteal*. 2015, http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.bankash.a.html.

[16] Barbieri, R., Bruschi, D and Rosti, E., *Voice over IPsec: analysis,*2012, [online]: available at www.securityresponsekaspersky.com/pwsteal.roshi.html

[17] Brar, T.P.S., Sharma, D and Khurmi, S.S., *Vulnerabilities in e-banking: A study of various security aspects in e-banking*, International Journal of the Internet of things, 2016, Vol. 5, No 3, pp 121 – 134.

[18] Chaturvedi, A and Meena, A., *Analysing the impacts of phishing and vishing attacks in Internet banking*, International Journal of Advanced Research in Computer Science and Software Engineering, 2016, Vol. 6, No. 3, pp 16 – 21.

[19] David, L., *Phishing expedition at heart of AT&T hacking*, San Francisco Chronicle, 2006.

[20] Davis, M., "*280 Kansas City employees fall for fake hack"*, 2015, [online]: available at www.kansascity.com/news/business/technology/article16376894.html, last retrieved July 2016

[21] Corrin, A., *Spear-phishing tactics becoming more sophisticated*, 2014, [online]: available at http://archive.federaltimes.com/article/20141024/CYBER/310240013/-Spear-phishing-tacticsbecoming-more-sophisticated

[22] Federal Bureau of Investigation., *Spear phishers*, 2009, [online] www.fbi.gov/news/stories/2009/april/spearphishing_040109.

[23] Ferguson, D., *Phishing warning Beware e-mails asking for personal info*, as cited in Yeboah-Boateng, E.O and Amanor, P.M., *Phishing, smishing and vishing: an assessment of threats against Mobile Devices*, Journal of Emerging Trends in Computing and Information Sciences, 2014, Vol. 5, No. 4, pp297-307

[24] Hong, J., *Why have there been so many security breaches recently*? 2015, http://cacm.acm.org/blogs/blog-cacm/107800-why-have-there-been-so-many-%security-breaches-recently/fulltext

[25] Johnson, M., *New approach to Internet Banking*, September 2008 Technical report (UCAM-CL-TR-731), Cambridge University, ISSN 1476-2986

[26] Korolov, M., *Omaha's Scoular company loses $17 million after spear phishing attack*, 2015, [online]: available at www.csoonline.com/article/2884339/malware-cybercrime/omahas-scoular-co-loses-17-million-after-spearphishing-attack.html

[27] Marko, J., *Larger preys are targets of phishing*, 2008, [online] http://www.nytimes.com/2008/04/16/echnology/16whale.html.

[28] FireEye, "*Spear Phishing Attacks – Why They are Successful and How to Stop Them: Combating the Attack of Choice for Cybercriminals*, 2012, [online]: www.crsonline.com/contents/security/reshsecurity.html.

[29] Firefox phishing protection bypass vulnerability. Securiteam, Jun 2006. http://blogs.securiteam.com/index.php/archives/467

[30] Gartner, Press Release, "*Gartner Says Worldwide data security Spending Will Grow 8-Percent in 2014 as organizations Become More Threat-Aware*", (August 22, 2014), http://www.gartner.com/newsroom/id/2828722

[31] Purkait, S., *Phishing counter measures and their effectiveness – literature review*, International Journal of Internet, 2015, Vol. 23, pp380-420.

[32] RSA, *A Year in Review*, http://www.emc.com/collateral/fraud-report/rsa-online-fraudreport-012014.pdf, 2014, last retrieved July 2016

[33] Waugh, R., "*Big Companies still fall for social engineering hacks by phone and it's not getting better*, 2013, http://www.welivesecurity.com/2013/10/31/big-companies-stillfall-for-social-engineering-hacks-by-phone-and-its-not-getting-better/

[34] Wang, X., Zhang, R., Yang, X., Jiang, X and Wijesekera, D., *Voice pharming attack and the trust of VoIP*, ACM Transaction on SecureCOMM, ISBN: 978-1-60558-241-2, 2008, Vol. 21, pp241-321.