Secure Mobile Banking

Hussam Elbehiery[1], M. Saied Abdelwahab[1], Ghada Abdelhady[2]

[1]Misr University for Science and Technology (MUST), Faculty of Information Technology, Egypt
[2]German University in Cairo (GUC), Faculty of Engineering, Egypt
hussam.elbehiery@gmail.com

Abstract: Most of banks have introduced the mobile banking service in many countries. Mobile banking is a system that allows customers of a financial institution to conduct a number of financial transactions through a mobile device such as a mobile phone or assistant. The introduced application has been created on a smart phone with the help of facial recognition and ciphering algorithms for increasing security. The aim of this application for bank customers is to perform banking transactions such as transferring money, paying bills and to make survey(s) on the users account through the mobile application wherever the user is and at any time. Many developed countries are using now the android application systems, so the introduced application mainly based on this operating system which becomes widely used all over the world in the smart phones.
[Hussam Elbehiery, M. Saied Abdelwahab, Ghada Abdelhady. **Secure Mobile Banking.** *J Am Sci* 2014;10(1):135-142]. (ISSN: 1545-1003). http://www.jofamericanscience.org. 22

Keywords: Mobile and Internet banking, Android operating system, Facial Recognition, and Ciphering Algorithms.

1. Introduction

Banks play an important role in moving the economic wheel with technological developments. [1] The Mobile Banking is a term used for performing Balance checks; Account transactions, Payments through money transfer, Credit applications, and various banking transactions.[2]

The most important services provided by the Bank mobile open an account, complete operations buying or selling, applying for credit cards, pay bills and transfer funds between accounts in the sense make cash transfers to any bank or any other account whether inside or outside the country. Mobile Banking is designed specifically for mobile devices, which means we use your device's built-in features to provide a better experience. The information is also formatted for display on smart phones.[3][4]

The Mobile Banking system proved to be achieving for the Bank profits up to 6 times the profit normal, because the Bank Mobile uses information technology to improve relations and expand the scope of its dealings with clients by dealing with personal data, which has about the customer an intelligent manner.[5][6]

For the marketing of its services, such as opening an account, get credit cards, pay bills, and transfer money between accounts.[7]

2. Mobile Banking services in Egypt

Egypt has a great potential to expand in retail banking activities due to its high population, electronic payment systems have developed over the last decade due to the rapid development of telecommunications and IT networks.[8] As early as 2000, a number of local and international banks launched electronic banking services to give clients access to cash and allow them to conduct necessary financial transactions. Yet, online banking services have not taken off in Egypt because of low rates of computer literacy and Internet penetration.

According to the Ministry of Communication and Information Technology (MCIT), the number of Internet users in Egypt was 35.95 million in 30 June 2012.[9,10] However, Egypt's Ministry of Communications and Information Technology National Telecom Regulatory Authority stated that the total number of mobile subscribers has already reached 96.77 million in July 2013. Also, the number of mobile Internet users has been reached 13.55 million in July 2013.[10]

Therefore, it is obvious that there is an upward trend in the Egyptian mobile usage. This brings a calling need for investing in Mobile Banking as it is a leading sector and mobiles are highly valued and used. Egyptian Mobile Banking has already taken its first steps from mere notification to actual transactions. In some banks customers can now pay for their mobile bills using their phones using SMS in Egypt. The success of m-banking in countries like South Africa, Kenya, and Botswana might also be an indication that Egypt's low-income segment may succeed too.[11,12,13]

Central Bank governor has announced that the standards for money transfers through mobile will be finalized within 6 months to start activating the new service. Some banks offer currently some mobile banking services Kalastalam balance, pay bills and transfer funds internally and messaging service over the phone, these banks are: -

- Egyptian Arab Aakary Bank
- National Societe Generale Bank (NSGB)

- Commercial International Bank (CIB)
- Arab Bank
- Bank of Egypt

3. Mobile Banking advantages & drawbacks

As in great banks which have large numbers of branches encourage the customers to use the system Bank Mobile and Internet which give multiple advantages such as effective time management and speed of response to service requirements, person client achievement, and conveying Mobile Banking services to client wherever.[14,15,16]

There are a number of drawbacks should be taken into account the service in banks suffer from including:[17,18,19]

- There is a kind of boom in IVR (Interactive Voice Response) method to merge with this service because the whole process is made through mobile phone.
- Preoccupation with the lines of communication at times, especially at peak times, which makes customers lose confidence in the service.
- The possibility of exposure of individuals to fraud as the mobile banking service across can be difficult to monitor accurately.

4. Face Recognition approaches

Face recognition approaches on still images can be broadly grouped into geometric and template matching techniques.[20] In the first case, geometric characteristics of faces to be matched, such as distances between different facial features, are compared. This technique provides limited results although it has been used extensively in the past. In the second case, face images represented as a two dimensional array of pixel intensity values are compared to a single or several templates representing the whole face.[21]

More successful template matching approaches use Principal Components Analysis (PCA) or Linear Discriminant Analysis (LDA) to perform dimensionality reduction achieving good performance at a reasonable computational complexity/time.[22] Other template matching methods use neural network classification and deformable templates, such as Elastic Graph Matching (EGM).[23] Recently, a set of approaches that use different techniques to correct perspective distortion are being proposed. These techniques are sometimes referred to as view-tolerant.

When the scenario departs from the easy scenario, then face recognition approaches experience severe problems. Among the special challenges let us mention: pose variation, illumination conditions, scale variability, images taken years apart, glasses, moustaches, beards, low quality image acquisition, partially occluded faces etc. An additional important problem to be recognized is how different face recognition systems are compared.

Therefore, there is an image processing system that has an impressive performance for all kind of scenarios: the human visual system (HVS).[24]

5. Ciphering

A cipher is an algorithm for performing encryption or decryption. In the online world encryption disguises data rearranging the data bits so that nobody can read or see the information without the secret key, this key can consist of a password or a digital file, aka key file, encryption secures plain text as well as any other digital media like photos, videos or software, you can also encrypt a whole operating system and a partition.[25]

There are two basic types of encryption schemes: Symmetric-key and public-key encryption. In symmetric-key schemes, the encryption and decryption keys are the same. Thus communicating parties must agree on a secret key before they wish to communicate. In public-key schemes, the encryption key is published for anyone to use and encrypt messages. However, only the receiving party has access to the decryption key and is capable of reading the encrypted messages. Public-key encryption is a relatively recent invention: historically, all encryption schemes have been symmetric-key (also called private-key) schemes.[25]

To secure data, encryption uses mathematic functions known as cryptography algorithms, aka ciphers, some example of well-known and trusted cryptography algorithms are AES, Blowfish, Twofish and Serpent, and these ciphers can be subcategorized with a number indicating its strength in bits.

An encryption algorithm key length indicates its size measured in bits, the length indicating the algorithm strength in bits will always be even (bit is binary unit composed of zeros and ones), these keys are used to control the operation of a cipher.

The more mathematical strength the encryption algorithm has the more difficult it will be to crack it without access to the key but a strong cipher normally requires more computational power, a few seconds of wait might not matter much to the home user but for businesses dealing with thousands of calculations each hour to decrypt/encrypt data in their servers it will mean that more money has to be spent in hardware and electricity.

6. Android operating system

Android is a Linux-based operating system designed primarily for touch screen mobile devices such as smart phones and tablet computers.[26]

Android become the world's most widely used smart phone platform and the software of choice for technology companies who require a low-cost,

customizable, lightweight operating system for high tech devices without developing one from scratch.

Android is developed in private by Google until the latest changes and updates are ready to be released, at which point the source code is made available publicly. This source code will only run without modification on select devices, usually the Nexus series of devices.[27]

Android manages the apps stored in memory automatically: when memory is low, the system will begin killing apps and processes that have been inactive for a while, in reverse order since they were last used (i.e. oldest first). This process is designed to be invisible to the user, such that users do not need to manage memory or the killing of apps themselves.[28]

Android 4.0 introduces a completely new approach to securing a device, making each person's device even more personal — Face Unlock is a new screen-lock option that lets you unlock your device with your face. It takes advantage of the device front-facing camera and state-of-the-art facial recognition technology to register a face during setup and then to recognize it again when unlocking the device. Just hold your device in front of your face to unlock, or use a backup PIN or pattern.[29]

7. Secure Mobile Banking application and implementation

FAINT; the face annotation interface is a flexible Java framework for face detection and face recognition technologies that is based on different plugin and filter types. A suitable graphical interface can be used to set up pipelines for detection and recognition by combining these plugins and filters. Moreover an integrated photo browser allows users to apply the face detection and recognition process on personal images.

It Includes Eigenfaces in pure Java, OpenCV detection via JNI, integration of the Betaface.com Web Service, skin color filter, Adobe XMP Export and a nice GUI.

The detected and recognized faces are stored in a local database, which can be modified manually from inside the application. In addition all face annotations can also be stored directly into the image files in Adobe XMP-Format on demand.

If all of the websites on the Internet used encrypted SSL connections the servers serving content using SSL (Secure Socker Layer) would need more CPU power and more electricity, when you multiply this by millions of pages served each second, costs dramatically add up, page loading would also be slower because the decryption process needs to take place in the computer and those using very low end processors in mobile devices would suffer speed the most.[25]

AES is a new cryptographic algorithm that can be used to protect electronic data. Specifically, AES is an iterative, symmetric-key block cipher that can use keys of 128, 192, and 256 bits, and encrypts and decrypts data in blocks of 128 bits (16 bytes). Unlike public-key ciphers, which use a pair of keys, symmetric-key ciphers use the same key to encrypt and decrypt data. Encrypted data returned by block ciphers have the same number of bits that the input data had. Iterative ciphers use a loop structure that repeatedly performs permutations and substitutions of the input data. Figure 5 shows AES in action encrypting and then decrypting a 16-byte block of data using a 192-bit key.[30,31]

An AES 128-bit encryption key is considered very strong and suitable to withstand future attacks, the U.S. Government requires 192 or 256-bit AES encryption keys for highly sensitive data, AES is the standard US Government encryption algorithm for data encryption.

A 128-bit key can have more than 300,000,000,000,000,000,000,000,000,000,000,000 key combinations.[32]

It is only a question of time before AES encryption becomes widely available from Microsoft and third-party vendors in the form of .NET Framework libraries. However, having this code in your skill set will remain valuable for a number of reasons. This implementation is particularly simple and will have low resource overhead. In addition, access to and an understanding of the source code will enable you to customize the AES class and use any implementation of it more effectively.

Security is no longer an afterthought in anyone's software design and development process. AES is an important advance and using and understanding it will greatly increase the reliability and safety of your software systems.[33]

Android 4.0 ice cream sandwich has been used for the introduced mobile banking application system. A good API (Application program interface) for that version makes it easier to develop a program by providing all the building blocks. Where the API level is a set of routines, protocols, and tools for building software applications.

As the starting of the application, the user enters the password of his/her account, if incorrect the user enters it again if correct it captures the image for image processing, when the picture is captured it is sent for correlation, then it is sent for comparison with the other pictures, if not identical the application goes out and starts from the beginning, if identical the user will entered to his/her account to perform bank transaction as shown in figure 1.

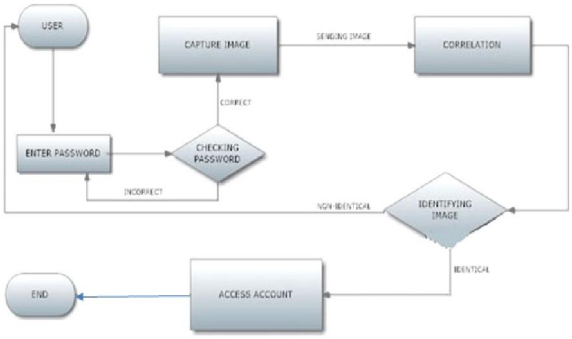

Figure 1. Secure Mobile Banking flowchart

In figure 2. The GUI of the software application on Android operating system smart phone has been seen.

Figure 2. Application interactive view on the Android O.S.

Here in the figure 3 and figure 4 the user is signing in for the mobile banking application with the help of facial recognition and his/her pin. The user enters his name, pin, e-mail, phone and the face photos to sign in then the process will begin.

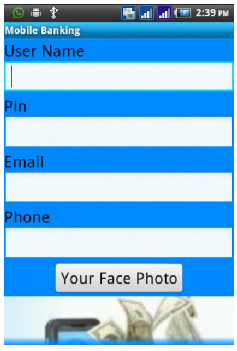

Figure 3. Interactive view for Sign in to the application

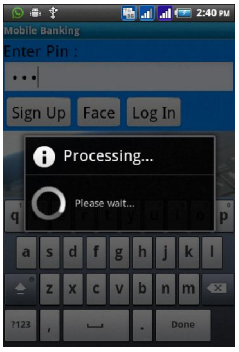

Figure 4. Interactive view for Sign in process starting

In the next step as seen in figure 5 the user take an image for him using mobile camera to transfer to the registering step.

Figure 5. Interactive view for taking the user image

The introduced Mobile Banking application is available for different banks as the user has many accounts on these banks. As the user select the bank he wants or wants to make an operation on the selected account the process will begin immediately as seen in figure 6.

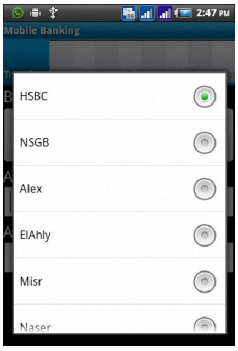

Figure 6. Interactive view for the bank account

One of the services introduced by the Mobile Banking application is the paying the bills online of the DSL or phones linked to all cell phone companies also the landline phone companies. In figures 7, and 8 which shows where the category (DSL or Phone), the

companies, the phone number and its confirmation for more security are used for the operation of paying bills.

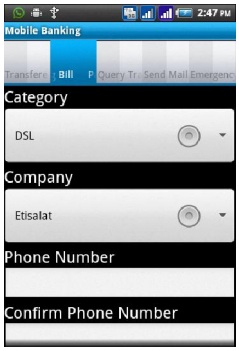

Figure 7. Interactive view for DSL and phones paying bills

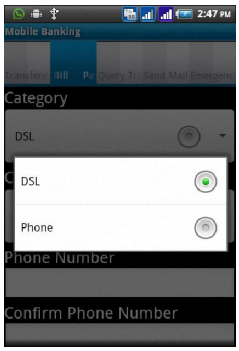

Figure 8. Interactive view for selecting the type of bills

In the next step; the user will select the company name from the list of the introduced companies supported by the Mobile Banking application to begin actually the bill payment. That will be seen in figure 9. The user will enter the phone number then confirm by enter again the phone number then fills the bill amount that should be paid which explained in figure 10.

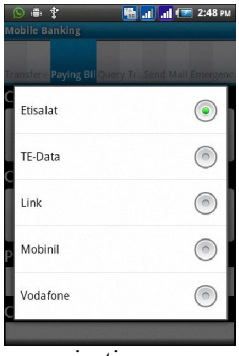

Figure 9. Telecommunication company selection interactive view

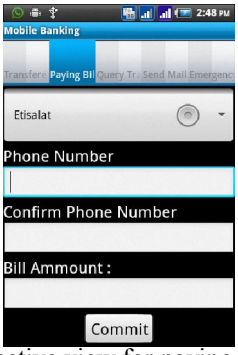

Figure 10. Interactive view for paying bill process

Here in figure 11 another service introduced by the Mobile Banking application which provides the Money transfer from bank account to another account.

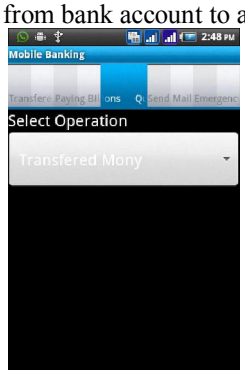

Figure 11. Money Transfer process interactive view

Here in figure 12 another service introduced by the Mobile Banking application which provides reviewing the last five operations of his/her banking transaction on the application.

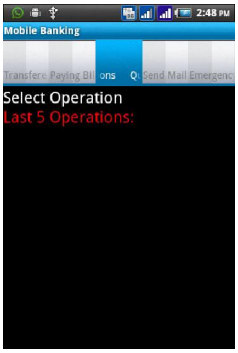

Figure 12. Interactive view for reviewing and listing the last five operations process

The user can send e-mail to the Bank server for any required information related or not related to the transactions via the service introduced by the Mobile Banking application which is seen in figure 13.

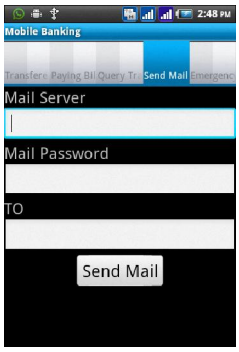

Figure 13. Interactive view for Bank's server correspondence process

The last service introduced by the Mobile Banking application is providing the user with high security to feel safe in case if the mobile stolen, lost, or hacked in just few minutes the account will be closed as shown in figure 14.

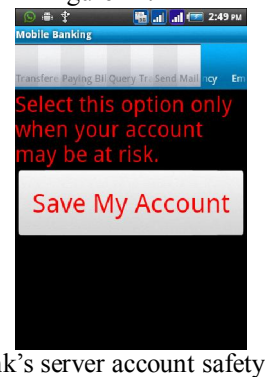

Figure 16. Bank's server account safety process interactive view

8. Software and Hardware Tools

8.1 Software tools

In this, research the software tools that are used:

- Eclipse (for java mobile applications).
- Android SDK (Software Development Kit).
- JDK (Java Development Kit).
- Java developer
- SQL
- "Faint" Image processing toolkit.

8.2 Hardware tools

The Hardware tools that are used:

- Smart phone (Samsung Galaxy DUOS using android system.
- Laptop

9. Conclusion

Each banking institution with online mobile access is starting to implement portals with the aim of seducing both clients and prospects by combining services that are accessible to all and functions that require valid authentication. And since mobile phones are continually being improved, the services on offer continue to evolve so that you can now perform a large number of tasks from your mobile phone as well as being able to freely manage your accounts when it best suits you.[34]

In the introduced secure mobile banking application, the main objective was to make the customer use the application to feel safe about his money during any transaction process he/she makes through the application. At the same time saves time and effort, besides the several services the application is offering which makes the customer indispensable to cooperate with bank branches.

Using Face recognition has been and will continue to be a very challenging and difficult problem. In spite of the great work done in the last 30 years, we can be sure that the face recognition research community will have work to do during, at least, the next 30 years to completely solve the problem. Strong and coordinated effort between the computer vision, signal processing and psychophysics and neurosciences communities are needed.

Acknowledgements

I would like to express my thanks to Misr University for Science and Technology – 6th October City - Cairo, Egypt for its affordable efforts in publishing this research paper also for providing necessary tools and kits and continuous support during the tests.

Corresponding Author:
Dr. Hussam Elbehiery
Head of Computer Science Department, Faculty of Information Technology, Misr University for Science and Technology, Giza, Egypt.
E-mail: hussam.elbehiery@gmail.com

References

1. Abd el Aziz, R., Beeson, I. and El Ragal, A., "An Empirical study to measure ATM usage in Egypt," IBIMA Proceedings, ISBN: 0-9753393-7-0, Dublin, Ireland, 2007.
2. Shrestha S., "Mobile web browsing: usability study," in Proceedings of the 4th international conference on mobile technology, applications, and systems and the 1st international symposium on Computer human interaction in mobile technology. Singapore: ACM, 2007, 187-194 International Journal of Managing Information Technology (IJMIT) Vol.3, No.4, November 2011.
3. Laukkanen, T., "Measuring mobile banking customers' channel attribute preferences in service consumption", International Journal of

Mobile Communications, Vol. 5 No. 2, pp. 123-38, 2007.
4. Suoranta, M. and Mattila, M., "Mobile banking and consumer behavior: New insights into the diffusion pattern", Journal of Financial Services Marketing, Vol. 4 No. 6, pp. 354-66, 2004.
5. Brown, I., Cajee, Z., Davies, D. and Stroebel, S. "Cell phone banking: predictors of adoption in South Africa – an exploratory study", International Journal of Information Management, Vol. 23 No. 5, pp. 381-94, 2003.
6. Sulaiman, A., Jaafar, N.I. and Mohezar, S., "An overview of mobile banking adoption among the urban community", International Journal of Mobile Communication, Vol. 5No. 2, pp. 157-68, 2007.
7. Pousttchi K. and Schurig M., "Assessment of today's Mobile Banking applications from the view of customer requirements", The 37th Hawaii International Conference on System Sciences, Big Island, Hawaii, January 5-8, 2004.
8. Rehaballah Elbadrawy and Rasha Abdel Aziz, "Resistance to mobile banking adoption in Egypt: a cultural perspective," International Journal of Managing Information Technology (IJMIT) Vol.3, No.4, pp. 9-21, November 2011.
9. Bandyopadhyay G., "Banking the Unbanked: Going Mobile in Africa" Principal Consultant, Infosys Technologies Ltd., 2010.
10. Arab Republic of Egypt Ministry of Communications and Information Technology, "ICT Indicators in Brief," July 2012 Monthly Issue,http://www.mcit.gov.eg/, http://www.egyptictindicators.gov.eg/.
11. Rajnish Tiwari and Stephan Buse, "The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Sector," Hamburg University Press, Hamburg, Germany, 2007.
12. Rajnish Tiwari, Stephan Buse, and Cornelius Herstatt, "Mobile Services in Banking Sector: The Role of Innovative Business Solutions in Generating Competitive Advantage," The International Research Conference on Quality, Innovation and Knowledge Management, New Delhi, India, pp. 886–894, 2007.
13. John Owens and Anna Bantug-Herrera, "Catching the Technology Wave: Mobile Phone Banking and Text-A-Payment in the Philippines," Chemonics International Inc., USA, 2006.
14. ArabCrunch, "Egypt's MCIT: Egypt Has 23.51 Million Internet Users, 71.46 Million Mobile Subscribers and 3972 ICT Companies," http://arabcrunch.com/2011/04/egypts-mcit-egypt-has-23-51-million-internet-users-71-46-million-mobile-subscribers-3972-ict-companies.html, April 2011.
15. Laukkanen, T., "Internet vs. mobile banking: comparing customer value perceptions", Business Process Management Journal, Vol. 13 No. 6, pp. 788-97, 2007.
16. Rajnish Tiwari, Stephan Buse, and Cornelius Herstatt, "Customer on the Move: Strategic Implications of Mobile Banking for Banks and Financial Enterprises," The 8th IEEE International Conference on E-Commerce Technology and The 3rd IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services (CEC/EEE'06), San Francisco, pp. 522–529, 2006.
17. Kuisma, T., Laukkanen, T. and Hiltunen, M., "Mapping the reasons for resistance to internet banking: a means-end approach", International Journal of Information Management, Vol. 27 No. 2, pp. 75-85, 2007.
18. Gerrard, P. Cunningham, J.B. and Devlin, J.F., "Why consumers are not using internet banking", Journal of Services Marketing, Vol. 20 No. 3, pp. 160-8, 2006.
19. Rajnish Tiwari, Stephan Buse, and Cornelius Herstatt, "Mobile Banking as Business Strategy: Impact of Mobile Technologies on Customer Behaviour and its Implications for Banks, in: Technology Management for the Global Future," Portland International Conference on Management Engineering and Technology (PICMET '06), July 8 – 13, USA, 2006.
20. W. Zhao, R. Chellappa, A. Rosenfeld and P.J. Phillips, "Face Recognition: A literature survey," Technical Report CART-TR-948. University of Maryland, USA, Aug. 2002.
21. Ming-Hsuan Yang, D.. Kriegman and N. Ahuja, "Detecting Faces in Images: A Survey", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, No. 1, pp. 34-58, January 2002.
22. S. Balakrishnama, A. Ganapathiraju, "Linear Discriminant Analysis - A Brief Tutorial," Institute for Signal and Information Processing proceeding, Department of Electrical and Computer Engineering, Mississippi State University, USA, 2005.
23. Stefanos Zafeiriou, and Maria Petrou, "2.5D Elastic graph matching," Computer Vision and Image Understanding journal, Elsevier, Volume 115, Issue 7, Pages 1062–1072, London, UK, July 2011.
24. I. Biederman, P. Kalocsai, "Neural and Psychophysical Analysis of Object and Face Recognition," Berlin, Springer-Verlag, pp. 3-25, 1998.

25. Konheim A., G., Konheim A., ”Cryptography: A Primer,” John Wiley and Sons, New York, 1981.
26. "Android Code Analysis" (http:/ / www. ohloh. net/ p/ android/ analyses/ latest). Retrieved 2012-06-01.
27. "Philosophy and Goals" (http:/ / source. android. com/ about/ philosophy. html). Android Open Source Project. Google. . Retrieved 2012-04-21.
28. Topolsky, Joshua, "Google's Android OS early look SDK now available" (http:/ / www. engadget. com/ 2007/ 11/12/googles-android-os-early-look-sdk-now-available/). Engadget, Retrieved 2012-02-17.
29. "Android 4.2.1 Jelly Bean heads to AOSP". Android Community. Retrieved 2012-11-27.
30. National Bureau of Standards, “Specifications for the Advanced Encryption Standard (AES),” http://csrc.nist.gov/publications/fips/fips197/fips-197, NBS, 2001.
31. Kaminsky, A., Kurdziel, M., and Radziszowski, S., “An overview of cryptanalysis research for the advanced encryption standard,” Military Communications Conference MILCOM’10, Pp: 1310 – 1316, San Jose, CA, USA, 2010.
32. Behran Bahrak and Mohammad Reza Aref., “A novel impossible differential cryptanalysis of AES,” Proceedings of the Western European Workshop on Research in Cryptology (WEWoRC’07), pages 152–156, 2007.
33. Behran Bahrak and Mohammad Reza Aref., “Impossible differential attack on seven-round aes-128,” IET Inf. Secur., 2(2):28–32, June 2008.
34. Hofstede, “Culture's Consequences, Comparing Values, Behaviors, Institutions, and Organizations across Nations,” Sage Publications; Second Edition; February 2003.

12/12/2013