Vulnerability Measures in Android OS

Dr.C. Nalini, H. Afroz

Abstract: Presently Smartphone's are essentially little PCs with included administrations, for example, GSM, radio. Consequently it is consistent with say that next eras of working framework will be on these Smartphone and any semblance of windows, IOS and android are demonstrating to us the look at this future. Android has as of now increased critical favorable circumstances on its partners regarding piece of the overall industry. One of the explanation for this is the most essential component of Android is that it is open-source which makes it free and permits any one individual could build up their own particular applications and distribute them uninhibitedly. This openness of android brings the engineers and clients an extensive variety of comfort yet at the same time it builds the security issues. The real danger of Android clients is Malware contamination through Android Application Market which is focusing on a few escape clauses in the design principally on the end-clients part. This paper exhibits the present condition of Android security systems and their restrictions additionally recognize certain security necessities.

Keywords: Android, Android security, Linux, mobile, smartphone, mobile security, mobile threats, Java.

INTRODUCTION

Android

Android is a cutting edge versatile stage that was intended to be genuinely open. Android applications make utilization of cutting edge equipment and programming, and additionally neighborhood and served information, uncovered through the stage to convey advancement and incentive to customers Developed by the Open Handset Alliance (obviously drove by Google), in view of Linux stage, Android is a broadly foreseen open source working framework for cell phones that gives a base working framework, an application middleware layer, a Java programming improvement unit (SDK), and a gathering of framework applications. The far reaching utilization of cell phones and its expanding functionalities has made both undertakings and customers to depend on these gadgets for their everyday life. This paper is sorted out as, first outline of android OS, its design and portrays the multi-layer structure which begins with a -Linux center, structure of android security and its vulnerabilities' and study the malware dangers show for the android OS. Impediment of security model, then at last eventual fate of android security.

Why is Mobile Security Important?

Mobile security or mobile phone security has become increasingly important in mobile computing. Of particular concern is the security of personal and business information now stored on smart phones.

More and more users and businesses use smart phones to communicate, but also to plan and organize their users' work and also private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks. Indeed, smart phones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company.

Android Security and Threats

A smart phone user is exposed to various threats when they use their phone. In just the last two quarters of the number of unique mobile threats grew by 261%, according to ABI Research. These threats can disrupt the operation of the smart phone, and transmit or modify user data.

Dr.C. Nalini, Professor, Department of Computer Science and Engineering, BIST, BIHER, Bharath Institute of Higher Education & Research, Selaiyur, Chennai. E-mail: nalini.cse@bharathuniv.ac.in

H. Afroz, PG Scholar, Department of Computer Science and Engineering, BIST, BIHER, Bharath Institute of Higher Education & Research, Selaiyur, Chennai. E-mail: afrozmumthu@gmail.com

So applications must guarantee privacy and integrity of the information they handle. In addition, since some apps could themselves be malware, their functionality and activities should be limited (for example: restricting the apps from accessing location information via GPS, blocking access to the user's address book, preventing the transmission of data on the network, sending SMS messages that are billed to the user, etc.)

ANDROID SECURITY ARCHITECTURE

Engineering With the enduring change in the android the essential Android System Architecture and Application structures continues as before as takes after:

- Robust security at the OS level through the Linux kernel Mandatory application sandbox for all applications
- Secure inter process communication
- Application signing
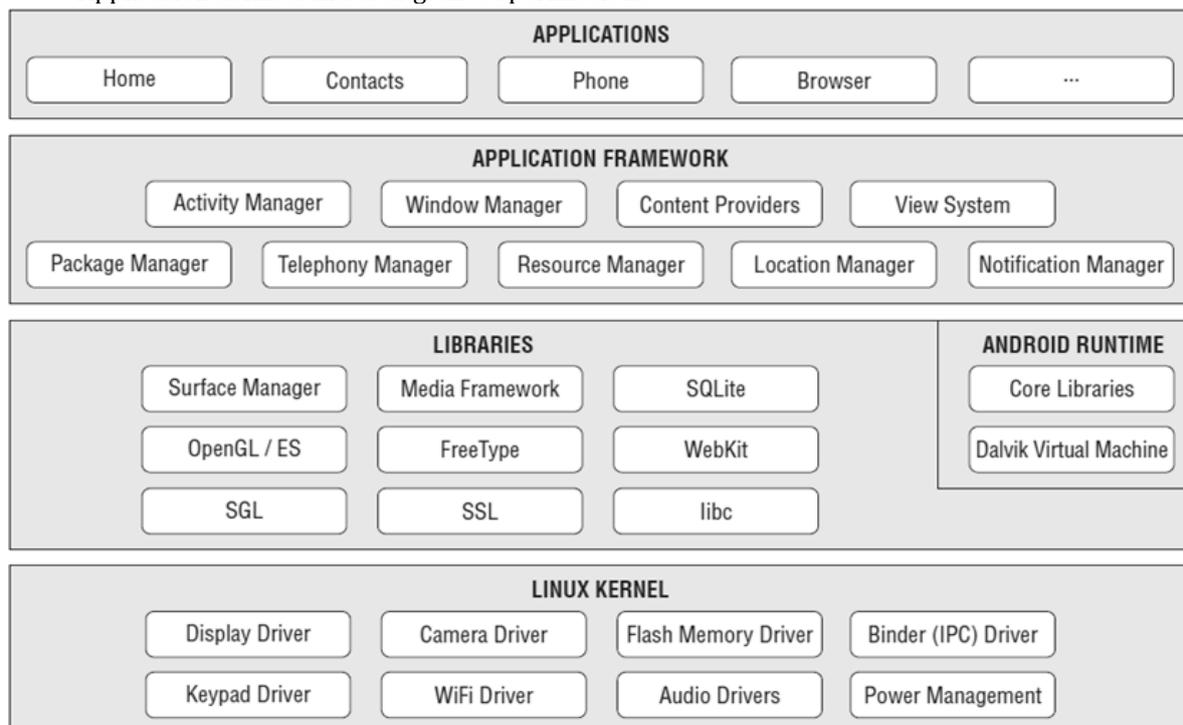- Application defined and user granted permissions

Figure 1: Android Architecture

Application Layer

The application segment of the Android working framework is the nearest to the end client. This is the place the Contacts, Phone, Messaging, and Angry Birds applications live. for example, Email Client, Web Browser and so on.

Application Framework Layer

This layer is produced particularly to allow designers full access to the center application structure utilized by the API. It comprises of a scope of administrations and framework structure which incorporate Active Manager, Windows Manager, View framework, Contents Provider, Package Manager, Resource Manage.

Libraries and Android Run-time Layer

This layer is predominantly connected with the procedure running. The center library gives a large portion of the elements of Java programming dialect.

The fourth layer - Linux portion

Kernel of Android is Linux 2.6 center which, Similar to a desktop PC running Linux, the Android piece will deal with power and memory administration, gadget drivers, prepare administration, systems administration, and security.

SECURITY ISSUE IN ANDROID

Data: smart phones are devices for data management, and may contain sensitive data like credit card numbers, authentication information, private information, activity logs (calendar, call logs);

Identity: smart phones are highly customizable, so the device or its contents can easily be associated with a specific person. For example, every mobile device can transmit information related to the owner of the mobile phone contract,[citation needed] and an attacker may want to steal the identity of the owner of a smart phone to commit other offenses;

Availability: attacking a smart phone can limit access to it and deprive the owner of its use.The source of these attacks are the same actors found in the non-mobile computing space Professionals, whether commercial or military, who focus on the three targets mentioned above. They steal sensitive data from the general public, as well as undertake industrial espionage. They will also use the identity of those attacked to achieve other attacks; Thieves who want to gain income through data or identities they have stolen. The thieves will attack many people to increase their potential income;

PROBLEM BASED OF ANDROID

As should be obvious the multi layer design of android each layer need to manage its on issue and there aversion instrument; for example, Android gives taking after security components to accomplish these goals by hearty security at the working framework level through the Linux part, a mandatory application sandbox for all applications, a Secure intervenes correspondence, Application consent system, and Application marking. Procedures of linux security, Dalviks JVM and application particular security mechanism are classified as takes after However, these counteractive action measures can be comprehensively arranged into 3 sorts

Benefit Separation (sandboxing)

The Android stage exploits the Linux client based security as a methods for distinguishing and detaching application assets. The bit actualizes a benefit partition show i.e. sandbox with regards to executing applications. This keeps other application from getting to the private data of the application. Unapproved access to equipment highlights like GPS, camera or system correspondence can be anticipated utilizing this sandboxing component.

Application Permission Mechanism

When putting in new application, Android prompts the client with the announced authorizations required by the application. The client must allow all the asked for authorizations, keeping in mind the end goal to introduce the application. The main probability for not giving the consents is not to introduce the application. Thus of conceding consent to an application, the application can get to the separate assets. In the present security show, it is impractical to give any beware of the use of an asset. This is a noteworthy confinement of current security demonstrate.

Application Code Signing

Any application that is to keep running on the Android working framework must be agreed upon. Android utilizes the declaration of individual designers with a specific end goal to recognize them and build up trust connections among the different applications running in the working framework. The working framework won't permit an unsigned application to execute. Any affirmation specialist to sign the testament is not required, and Android will cheerfully run any application that has been marked with a self-marked declaration.

RESTRICTIONS IN ANDROID SECURITY

Cell phone is security is to some degree delicate theme than our ordinary PC assurance in light of the fact that the straightforward truth that the information on our telephone is more vital to utilize and contain more essential information to the, henceforth the User should be more mindful about the impediment of the present security display. The android sandbox is application particular it educate client about the authorization they require client can acknowledge or dismiss however the dismissal implies not establishment. The real drawback to mark instrument is that an engineer can distribute application to the Android showcase after a self-marking. As nonattendance of focal of expert this does not require any ensuring specialist i.e., engineer can utilize self-made declarations to sign their applications.

A portion of the vulnerabilities in the current authorization demonstrate emerge from the idea of shared client ID system.

The common client ID include permits one application to use the allowed authorizations to another application having a similar client ID. As it were the point at which an application with a common client ID is introduced on the cell phone, the majority of its conceded authorizations are credited to the client ID.

In any case, numerous applications accessible in the Android advertise have announced both the consents paying little heed to their need of these authorizations that can prompt to conceivable abuse of the individual assets.

A portion of the vulnerabilities like battery depleting, Denial of Service assaults (DoS) and Distributed Denial of Service assaults (DDoS) i.e., denying to place telephone calls to nonemergency numbers, application end, and the abuse of billable administrations, for example, MMS/SMS messages and telephone calls, and so forth., are cases of a portion of the unmistakable assaults on advanced cells.

ADAVANTAGES & DISADVANTAGES OF ANDRIOD OS

ADVANTAGES OF ANDROID OS

It supports various platforms like 2D and 3D. Earlier we used to watch movies and play games in almost in 2D, but nowadays various applications are using 3D format. To provide different graphics in videos, games OS should support 3D format. Android supports 2D And 3D format to provide a better advantage in videos and in games.

Java Support

The Java supporting feature enables developers to enhance more features. As it supports Java, operating can be developed

Video Calling

Faster data connection enables to do video call. We can take advantage of bandwidth and new generation networks using Android.

Availability of Apps

Anyone can make use lot of free apps in the app store and from other android stores. It gives freedom to install from third party users.

At a Time Applications

Can run numerous applications which allow consumers to help save time and efforts

Disadvantages of Android OS

Slow response

Compared to 'ios' of apple, windows 8 of Microsoft.when we open same app in the ios and windoes8. We observe the slow response of the android when we open apps in the different platforms.

Heat

Compared to other operating systems android makes use of processes very efficient. This makes processor to get heat. Some hardware companies take care to reduce heat,but it went in vain when we operate it a long time and at low battery.

Advertisement

When we use an android app we encounter several adds in between application use, because anyone can make add by inserting some logic in the app program and can interfere in into the phones information.

This is all about android operating system and the advantages of android operating system, which made tremendous changes in last five years. Almost every smart phone, tablet and electronic device using android operating system. It is user friendly and open source to develop.

SUMMARY

The developing prominence of advanced cell use and its wide selection in the market has offered ascend to essential security concerns. This paper breaks down the security component the most generally utilized open source advanced mobile phone stage Android. Examined security instruments and there

constraint. Malware are the significant danger to the android client, the most ideal approach to keep away from them is to make client mindful of the security component and how to utilize them in his advantage and stop malwares at their establishment stage.

REFERENCES

[1] Udayakumar, R., Khanaa, V., & Saravanan, T. (2013). Analysis of polarization mode dispersion in fibers and its mitigation using an optical compensation technique. *Indian Journal of Science and Technology*, *6*(6), 4767-4771.

[2] Udayakumar, R., Kumaravel, A., & Rangarajan, K. (2013). Introducing an efficient programming paradigm for object-oriented distributed systems. *Indian Journal of Science and Technology*, *6*(5S), 4596-4603.

[3] Mageswaran, S.U., & Sekhar, N.G. (2013). Reactive power contribution of multiple STATCOM using particle swarm optimization. *International Journal of Engineering & Technology*, *5*(1), 122-126.

[4] Giri, R.K., & Saikia, M. (2013). Multipath routing for admission control and load balancing in wireless mesh networks. *International Review on Computers and Software*, *8*(3), 779-785.

[5] Padmapriya, G., Manikandan, A., Krishnasamy, V., Jaganathan, S.K., & Antony, S.A. (2016). Spinel NixZn1− xFe2O4 (0.0≤ x≤ 1.0) nano-photocatalysts: synthesis, characterization and photocatalytic degradation of methylene blue dye. *Journal of Molecular Structure*, *1119*, 39-47.

[6] Vijayaragavan, S.P., Karthik, B., Kiran Kumar, T.V.U., & Sundar Raj, M. (2013). Analysis of chaotic DC-DC converter using wavelet transform. *Middle-East Journal of Scientific Research*, *16*(12), 1813-1819.

[7] Lokesh, K., Kavitha, G., Manikandan, E., Mani, G.K., Kaviyarasu, K., Rayappan, J.B.B., ... & Maaza, M. (2016). Effective ammonia detection using n-ZnO/p-NiO heterostructured nanofibers. *IEEE Sensors Journal*, *16*(8), 2477-2483.

[8] Abraham, A.G., Manikandan, A., Manikandan, E., Vadivel, S., Jaganathan, S.K., Baykal, A., & Renganathan, P.S. (2018). Enhanced magneto-optical and photo-catalytic properties of transition metal cobalt (Co2+ ions) doped spinel MgFe2O4 ferrite nanocomposites. *Journal of Magnetism and Magnetic Materials*, *452*, 380-388.

[9] Kennedy, J., Fang, F., Futter, J., Leveneur, J., Murmu, P.P., Panin, G.N., & Manikandan, E. (2017). Synthesis and enhanced field emission of zinc oxide incorporated carbon nanotubes. *Diamond and Related Materials*, *71*, 79-84.

[10] Teresita, V.M., Manikandan, A., Josephine, B.A., Sujatha, S., & Antony, S.A. (2016). Electromagnetic properties and humidity-sensing studies of magnetically recoverable LaMg x Fe 1− x O 3− δ perovskites nano-photocatalysts by sol-gel route. *Journal of Superconductivity and Novel Magnetism*, *29*(6), 1691-1701.

[11] Caroline, M.L., & Vasudevan, S. (2009). Growth and characterization of pure and doped bis thiourea zinc acetate: Semiorganic nonlinear optical single crystals. *Current applied physics*, *9*(5), 1054-1061.

[12] Jayalakshmi, V., & Gunasekar, N.O. (2013). Implementation of discrete PWM control scheme on Dynamic Voltage Restorer for the mitigation of voltage sag/swell. *International Conference on Energy Efficient Technologies for Sustainability*, 1036-1040.

[13] Udayakumar, R., Khanaa, V., & Kaliyamurthie, K.P. (2013). Optical ring architecture performance evaluation using ordinary receiver. *Indian Journal of Science and Technology*, *6*(6), 4742-4747.

[14] Udayakumar, R., Khanaa, V., & Kaliyamurthie, K.P. (2013). Performance analysis of resilient ftth architecture with protection mechanism. *Indian Journal of Science and Technology*, *6*(6), 4737-4741.

[15] Saravanan, T., Srinivasan, V., & Sandiya, V.P. (2013). A two stage DC-DC converter with isolation for renewable energy applications. *Indian Journal of Science and Technology*, *6*(6), 4824-4830.

[16] Sundarraj, M. (2013). Study of compact ventilator. *Middle-East Journal of Scientific Research*, *16*(12), 1741-1743.

[17] Thema, F.T., Manikandan, E., Gurib-Fakim, A., & Maaza, M. (2016). Single phase Bunsenite NiO nanoparticles green synthesis by Agathosma betulina natural extract. *Journal of alloys and compounds*, *657*, 655-661.

[18]   Sathyaseelan, B., Manikandan, E., Sivakumar, K., Kennedy, J., & Maaza, M. (2015). Enhanced visible photoluminescent and structural properties of ZnO/KIT-6 nanoporous materials for white light emitting diode (w-LED) application. *Journal of Alloys and Compounds*, *651*, 479-482.

[19]   Gopalakrishnan, K., Prem Jeya Kumar, M., Sundeep Aanand, J., & Udayakumar, R. (2013). Analysis of static and dynamic load on hydrostatic bearing with variable viscosity and pressure. *Indian Journal of Science and Technology,* 6(6), 4783-4788.

[20]   Prabhu, M.R., Reji, V., & Sivabalan, A. (2012). Improved radiation and bandwidth of triangular and star patch antenna. *Research Journal of Applied Sciences, Engineering and Technology*, *4*(12), 1740-1747.

[21]   Arumugam, S. and Ramareddy, S. (2012). Simulation comparison of class D/ Class E inverter fed induction heating. *Journal of Electrical Engineering*, 12(2), 71-76.

[22]   Udayakumar, R., Khanaa, V., & Kaliyamurthie, K.P. (2013). High data rate for coherent optical wired communication using DSP. *Indian Journal of Science and Technology*, *6*(6), 4772-4776.

[23]   Nagarajan, C., & Madheswaran, M. (2012). Experimental Study and Steady State Stability Analysis of CLL-T Series Parallel Resonant Converter with Fuzzy Controller using State Space Analysis. *Iranian Journal of Electrical and Electronic Engineering*, *8*(3): 259-267.

[24]   Gopalakrishnan, K., PremJeya Kumar, M., SundeepAanand, J., & Udayakumar, R. (2013). Thermal properties of doped azopolyester and its application. *Indian Journal of Science and Technology*, *6*(6), 4722-4725.

[25]   Kumaravel A., Meetei O.N. (2013). An application of non-uniform cellular automata for efficient cryptography. *Indian Journal of Science and Technology*, *6*(5): 4560-4566.

[26]   Kumaravel, A., & Pradeepa, R. (2013). Layered approach for predicting protein subcellular localization in yeast microarray data. *Indian Journal of Science and Technology*, *6*(5S), 4567-4571.

[27]   Kaviyarasu, K., Manikandan, E., Kennedy, J., & Maaza, M. (2016). Synthesis and analytical applications of photoluminescent carbon nanosheet by exfoliation of graphite oxide without purification. *Journal of Materials Science: Materials in Electronics*, *27*(12), 13080-13085.

[28]   Mathubala, G., Manikandan, A., Antony, S.A., & Ramar, P. (2016). Photocatalytic degradation of methylene blue dye and magneto-optical studies of magnetically recyclable spinel NixMn1-xFe2O4 (x= 0.0–1.0) nanoparticles. *Journal of Molecular Structure*, *1113*, 79-87.

[29]   Manikandan, E., Kennedy, J., Kavitha, G., Kaviyarasu, K., Maaza, M., Panigrahi, B.K., & Mudali, U.K. (2015). Hybrid nanostructured thin-films by PLD for enhanced field emission performance for radiation micro-nano dosimetry applications. *Journal of Alloys and Compounds*, *647*, 141-145.

[30]   Kumaravel, A., & Meetei, O.N. (2013). An application of non-uniform cellular automata for efficient cryptography. *IEEE Conference on Information & Communication Technologies*: 1200-1205.

[31]   Annie, J.P., Dr. Paul, S., & Dr. Ponmary Pushpalatha, D. (2014). Decision Tree Analysis to Predict Traffic Congestion in Transport Routing. *International Scientific Journal on Science Engineering & Technology, 17*(10), 905-910.

[32]   Asha, R.S., & Dr.Jayasree V.K., (2015). Simulative Investigation of Coherent Optical OFDM Communication with Gbits/s Data Rates. *Bonfring International Journal of Research in Communication Engineering, 5*(3), 22-26.

[33]   Tsai, C.I., & Lo, C.H., (2014). Integrating Phosphorylation and Catalytic Sites Information into AH-DB. *The SIJ Transactions on Computer Science Engineering & its Applications, 2*(4), 54-58.

[34]   Bhasker, B., & Dr.Murali, S. (2019). Networks Flaws and Filtering Using KNOD Algorithms. *Bonfring International Journal of Software Engineering and Soft Computing, 9*(2), 36-39.

[35]   Chávez, J.J.G., & Rodrigues, C.K.D.S. (2015).A Simple Algorithm for Automatic Hopping among Pools in the Bitcoin Mining Network. *The SIJ Transactions on Computer Networks & Communication Engineering (CNCE), 3*(1), 6-11.

[36]   Beena Ullala Mata, B.N., & Dr. Meenakshi, M. (2018). Mammogram Image Segmentation by Watershed Algorithm and Classification through k-NN Classifier. *Bonfring International Journal of Advances in Image Processing, 8*(1), 01-07.

[37]   Dr.Prabavathy, K. (2018). Enhanced Information Retrieval System (E-IRIS) for Named Entity Recognition. *Journal of Computational Information Systems, 14*(3), 108 - 112.

[38]   Maalini, D., & Balraj, E. (2018). Secured and Energy Efficient Packet Transmission in Wireless Sensor Networks using Flooding protocol and AES Algorithm. *Journal of Computational Information Systems, 14*(4) 7 - 13.

[39]   Dr.Kathirvelu, M., Sethuramalingam, N., Vignesh, M., Vijayakumar, K., & Vasudevamoorthy, L.(2015). Low Cost Music Mixture Module for Entertainment Industry. *International Journal of Advances in Engineering and Emerging Technology, 7*(3), 152-155.

[40]   Chandrakala, K., Meenakshy, L., Nivedha, S., Priyanka, P., & Punithalakshmi, R. (2015). A Cross Layer Based Modern Handover Algorithm for Mobile WiMAX. *International Journal of Advances in Engineering and Emerging Technology, 7*(4), 225-236.

[41]   Langeswaran, K., Gowthamkumar, S., Vijayaprakash, S., Revathy, R., & Balasubramanian, M.P. (2013). Influence of limonin on Wnt signalling molecule in HepG2 cell lines. *Journal of natural science, biology, and medicine*, *4*(1), 126-133.

[42]   Srinivasan, V., & Saravanan, T. (2013). Analysis of harmonic at educational division using CA 8332. *Middle-East Journal of Scientific Research*, *16*(12), 1768-73.

[43]   Josephine, B.A., Manikandan, A., Teresita, V.M., & Antony, S A. (2016). Fundamental study of LaMg x Cr 1– x O 3– δ perovskites nano-photocatalysts: sol-gel synthesis, characterization and humidity sensing. *Korean Journal of Chemical Engineering*, *33*(5), 1590-1598.

[44]   Saravanan, T., Saritha, G., & Udayakumar, R. (2013). Robust H-Infinity Two Degree of Freedom Control for Electro Magnetic Suspension System. *Middle-East Journal of Scientific Research*, *18*(12), 1827-1831.

[45]   Rajasulochana, P., Dhamotharan, R., Murugakoothan, P., Murugesan, S., & Krishnamoorthy, P. (2010). Biosynthesis and characterization of gold nanoparticles using the alga Kappaphycus alvarezii. *International Journal of Nanoscience*, *9*(05), 511-516.

[46]   Slimani, Y., Güngüneş, H., Nawaz, M., Manikandan, A., El Sayed, H. S., Almessiere, M. A., & Baykal, A. (2018). Magneto-optical and microstructural properties of spinel cubic copper ferrites with Li-Al co-substitution. *Ceramics International*, *44*(12), 14242-14250.

[47]   Kaviyarasu, K., Manikandan, E., Kennedy, J., Jayachandran, M., & Maaza, M. (2016). Rice husks as a sustainable source of high quality nanostructured silica for high performance Li-ion battery requital by sol-gel method–a review. *Adv. Mater. Lett*, *7*(9), 684-696.

[48]   Ilayaraja, K., & Ambica, A. (2015). Spatial distribution of groundwater quality between injambakkamthiruvanmyiur areas, south east coast of India. *Nature Environment and Pollution Technology*, *14*(4), 771-776, 2015.

[49]   Sharmila, S., Rebecca, L. J., Das, M.P., & Saduzzaman, M. (2012). Isolation and partial purification of protease from plant leaves. *Journal of Chemical and Pharmaceutical Research*, *4*(8), 3808-3812.

[50]   Rajakumari, S.B., & Nalini, C. (2014). An efficient cost model for data storage with horizontal layout in the cloud. *Indian Journal of Science and Technology*, *7*(3), 45-46.