IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

Review of Mobile Security Risk Assessment on Smartphone

Dr. Y. Kalpana[1] and Dr. K. Kasturi[2]
[1]Professor & [2]Associate Professor Department of Applied Computing and Emerging Technologies,
VELS Institute of Science Technology and Advanced Studies, Chennai, India
kalpana.scs@vistas.ac.in[1], kasturi.scs@vistas.ac.in[2]

Abstract: *Mobile security is the protection of smart phones, tablets, laptops and another portable computing devices. The mobile security has been chosen due to the rise in mobile applications. Mobile devices are considered as tablet and cell phones which run a mobile Operating System. Specifically, Android (google), IOS(Apple),BlackBerry(RIM). Mobile security is focused primarily on the Android OS security vulnerabilities. Number of vulnerabilities and hence, of attacks increase, there has been a corresponding rise of security solutions proposed by researchers. We provide the overview of the research on security solutions for mobile devices. The risk evaluation utilizes two methodologies, security design level appraisal, and delicate information chance appraisal. Security setup level appraisal depends on implicit Android Smartphone arrangements, while touchy information chance evaluation depends on a blend of consents from all applications introduced on the devise.*

Keywords: Mobile, Security, Smart phones, Android, IOS, Blackberry, Google, Vulnerability, Information system, HIS.

I. INTRODUCTION

Mobile security is the protection of smart phones, tablets, laptops and other portable computing devices, and the networks they connect to, from threats and vulnerabilities associated with wireless computing. Mobile security is also known as wireless security. Verizon Support & Protection is an app that helps to better manage our smart phone. Android app users can lock their device, erase its contents and protect it from viruses or Malware Protection. Norton Mobile Security offers a straightforward set of anti-malware features. We can scan manually or set scans (quick or full) to run daily, weekly or monthly. The app is always monitoring installations and updates for malware. Mobile authentication may be used to authorize the mobile device itself or as a part of a multifactor authentication scheme for logging into secure locations and resources. Password entry is clumsy on cell phones, especially when including capital letters, numbers and symbols. Some alternative methods of mobile authentication include:

- Non-text passwords, where symbols or images might be chosen from a randomly-generated field.
- Digital certificates using public key infrastructure.
- Smartcards with stored authentication data.
  Out of band authentication, where the user places a call to obtain authentication.
- Time passwords One (OTP) through phone apps or SMS messages.
  Mobile authentication is the verification of a user's identity through the use of a mobile device and one or more authentication methods for secure access.

II. LITERATURE SURVEY:

Network security monitoring and defense system framework design using mobile agents based on dodaf by yan tong, jian zhang, tao qin, ming-di xu in 2015,Proposed the conventional system security checking frameworks more often than not utilize bunches of operators to gathered information and after that perform anomalous recognition in view of estimation of those information. This sort of structure needs loads of specialists and more often than not possesses

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

numerous data transfer capacities. Concentrate on this issue; we bring the portable specialists into the system security and checking framework. As the portable specialists are insightful and can move to different hosts as indicated by the checking undertaking, selection of the versatile operators will expand the adaptability of the observing framework while lessen the quantity of specialists. We additionally examined the components incorporated into the customary system security checking framework and mapped them to DM2.Based on those mapping works, we can get DM2 which ought to be incorporated into various perspectives in DoDAF. We get the creating succession of those perspectives and outline and build up the system security checking and safeguard framework structure utilizing the portable specialist .Based on EA, we confirmed the composed system and the outcomes demonstrate that the proposed system is right. DoDAF to make the outlined structure all the more effectively utilized and conveyed. We isolated the outlined design into four sections in view of the TOGAF.

Security in cloud-computing-based mobile health By Silas L. Albuquerque and Paulo R.L. Gondim , proposed the data security region, worries about the security of patients' wellbeing information, for instance, were limited in conventional human services IT situations to measures that ensured information found just on the wellbeing associations' PCs. The utilization of distributed computing has made such worries much more mind boggling, and we should now consider the security of data here and there put away in situations that are internationally open. This innovation happened, as it were, to free individual gadgets from requiring substantial capacity or handling limits—rather, these components could be exchanged to the cloud. Regardless of these prerequisites, one of the greatest focal points of m-wellbeing engineering is its adaptability in empowering the formation of wellbeing checking administrations that aren't constrained to customary human services conditions, for example, doctor's facilities or centers. Helped patients, for this situation, can be found at home, work, or somewhere else through a remote association with the correspondences organizes. The idea of m-wellbeing is no specific and envelops correspondence systems, versatile processing, medicinal sensors, and other human services related advancements. Distributed computing stockpiling and preparing abilities has offered ascend to versatile distributed computing (MCC).A WBASN must meet different suppositions with the goal that it satisfies its motivation in the m-wellbeing setting.

Mobile agent based security in manets against sybil attack by A.Aranganathan, C.D.Suriyakala in 2014, proposed An assault in MANET is exceptionally powerless for every one of the layers. An assault goes about as a noxious hub which influences the system execution. Sybil assault is one of the extreme assaults in system layer which makes disarray in the steering which can be identified and counteracted by an Agent. Specialist can ready to refresh the directing data all through the system and furthermore to diminish the system stack. The enhanced in the bundle conveyance proportion, decreased system over-burden and the enhanced data transmission productivity are performed utilizing ns2 apparatus. It is a sort of remote systems that are self-composed and progressively reconfigurable with no foundation or no settled base stations. MANETs are portrayed by element topologies, data transmission compelled, variable limit connections and vitality obliged operation, which represent a major test for the outline of proficient steering conventions for such systems. In a MANET, a gathering of portable terminals regularly cooperate to play out a specific undertaking. There are a different number of steering conventions which can do the typical operation. Portable specially appointed systems (MANETs).We takes the multicast directing convention as ODMRP.

Towards cloud-based compositions of security functions for mobile devices By ga¨etan Hurel, R´emi Badonnel, Abdelkader Lahmadi and Olivier Festor proposed another way to deal with outsource versatile security capacities and construct straightforward in-way security organizations for cell phones. The capacities are progressively enacted, arranged and formed utilizing programming characterized systems administration and virtualization abilities. We show a numerical formalization to demonstrate the security sytheses, and depict the useful design. We give a usage model and assess the arrangement through a broad arrangement of trials. The greater part of portable security arrangements are accessible as applications to be specifically introduced on the gadgets themselves. Such on-gadget approaches offer a few favorable circumstances yet actuate for the most part noteworthy assets utilization on the framework, prompting to the decrease of the battery lifetime. Meanwhile, current cloud-based arrangements attempt to offload the vast majority of the workload on remote servers, while just requiring lightweight operators to be introduced on the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 20, April 2026 Impact Factor: 8.2

frameworks. Such arrangements decrease the measure of utilized assets on the gadgets, yet no less than two noteworthy issues remains Companies are continuously moving from conventional client provided gadgets to BYOD1-related strategies. NFV-like virtualization and distinctive Open stream based, DNS-based redirection components.

Confidentiality and privacy information security risk assessment for android-based mobile devices by Irwan, Yudistira Asnar1, Bayu Hendradjaya in 2015.proposed an Android consent based security model are utilized to confine the capacity of uses to get to gadget assets, yet it neglected to give a sufficient control to clients and a perceivability of how outsider applications utilizing individual information of clients. The authorization notices when introducing applications don't help most clients in taking right security choices. This exploration goes for building up a hazard appraisal technique to decide security act, at Android Smartphone. The technique can help clients to expand the security level of a gadget, particularly against delicate information spillage. The outline of hazard appraisal utilizes two methodologies, security arrangement level evaluation and touchy information chance assessment. Security setup level appraisal depends on implicit Android Smartphone designs, while delicate information chance appraisal depends on mix of authorizations from all applications introduced on the gadget. Plan of hazard appraisal actualized on Android Smartphone called Smartphone Risk Assessment (SRA). The assessment has been finished by an ease of use testing utilizing the System Usability Scale (SUS) poll. The outcome demonstrates that the SRA is evaluated as "Great" by respondents in view of SUS score. The SRA is thought to be useful by clients to decide potential dangers of their advanced mobile phones and any applications that can possibly release delicate data. Risk Assessment, Smartphone's, Android, Sensitive Data, and Security. The plan of hazard evaluation that is executed on Android Smartphone is called SRA (Smartphone Risk Assessment).

Android mobile based home security and device control using gsm by s. Rajadurai, p. P. Nehru, r. Selvarasu in 2015,proposed The framework can impel a stick to bolt or open an entryway from a short separation away with the push of a catch on the cell phone. It could likewise check the status of the entryway. It is likewise to be a short range framework that is easy to utilize. The range and security viewpoints are accomplished using the on board Bluetooth radio of the cell phone. This framework utilized home robotization strategy. The cell phone could likewise control any apparatuses incorporated into the keen home framework through. The first program model for both the cell phone and the microcontroller just imparted a solitary character to flip a LED on the microcontroller proto board. The cell phone UI comprised on a solitary catch to transmit the character in light of the fact that the MAC address of the microcontroller was hard coded in.

A logic-based security framework for mobile perimeter by Mahesh Nath Maddumala in 2015,proposed theroutine approach of building, actualizing and overseeing firewalls for giving solid security to portable (remote) streams. The thought to stop assaults through area particular approach is very imaginative. This framework is reference design, numerical structure to indicate approaches for planning and progressively altering channels, their proficient usage, area particular message sifting, and polynomial math for creating and proliferating changes to such strategies for wired and versatile frameworks. Not able to respond to changes in its outside condition and they have physical constraints and contrasts in trust connections. Security structures give building answers for firewall insurance and show up profoundly framework subordinate. They are not adaptable and not powerfully self-altering.

Security framework for portable nfc mobile based health record system by divyashikha sethia, daya gupta, huzur saran in 2016 proposed the intermediary based cp-abe(ciphertext attribute-based encryption) plan is utilized for RBAC(Role-Based Access Control) with particular read and compose access to different areas on the healthcard and gives classification, trustworthiness and security of the patient. It can give exceedingly accessible and solid wellbeing records for proficient treatment. The testing comes about show that the timings for common validation, correspondence and decoding are middle of the road for a safe association amongst patient and medicinal expert. The constraint of space we exhibit nitty gritty outline for the Role Based Access Policy (RBAC) with particular read and compose get to include. Distinctive approved therapeutic experts get to it by simply tapping healthcard to their cell phone, utilizing low vitality remote correspondence interfaces, for example, NFC (Near field correspondence) and Bluetooth.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 20, April 2026 Impact Factor: 8.2

Cloud platform based automated security testing system for mobile internet by dan tao, zhaowen lin, and cheng lu in 2015 Proposed The trial comes about demonstrate that this framework can accurately test both the quantity of defenseless applications and their comparing helplessness levels. The planned framework can adaptably arrange different testing situations for various testing cases or extends, and accordingly perform security testing consequently. This framework utilized procedures are robotized trying strategy, virtualization and mechanization innovation. The sign strategy used to guarantee unapproved individual can't change the first information or data that sent through the system. Contrasted with the customary Internet, the wellsprings of danger for the portable Internet are more extensive and nature is more unpredictable. The developing security issue is mostly because of elements, for example, versatile terminal security gaps, basic system assaults, defenseless TCP conventions, et cetera.

Efficient message security based hyper elliptic Curve cryptosystem (hecc) for mobile instant messenger, by Putra Wanda, Selo, Bimo Sunafri Hantono in 2014,the proposed system to enhance the verification strategy for proficient correspondence in 1M(Instant Messenger). An effective validation technique will execute Hyper Elliptic Curve Cryptosystem (HECC) calculation in creating and checking the message sign while happen information exchange. Information verification with an advanced mark technique which have great security level, low computational, quick encryption. The primary capacity of marking message is to verify information to guarantee approval of information. Most clients jump at the chance to utilize straightforward and short passwords. Unapproved individuals can without much of a stretch split the basic passwords and making assault. Open key calculations will require huge memory and long time enough, for this issue calculation decision turn into an answer for mitigate overhead.

Routing and data security scheme based on double encryption in mobile ad hoc networks by Xuewen Wu, Xiaokai Zhu, Fei Kong in 2015, proposed the Solid practicability and is qualified to be generally spread, and higher execution. Bring down unpredictability and overhead, it can be embraced in all directing conventions to shield security assault of the course and information. Worldwide Mobile Information System Simulator (GloMoSim) apparatus and assess their execution utilizing the measurements, for example, normal end-to-end delay, normal bundle conveyance portion and normal steering control cost. Twofold encryption unraveled the directing and information security issues brought by false course assault and it would better ensured the parcel conveyance. MANETs has a considerable measure of secure issues, for example, dynamic changing of topology, unfixed wellbeing offices, free and open system condition and delicate remote channels, particularly the security issue of steering and information. MANETs are extremely perplexing, different and hidden; it is difficult to play it safe. Steering security and information security issues in MANETs. Information transmission transfers on the course yet their system capacities are autonomous generally and secure issues are distinctive and directing security and information security issues in MANETs. Higher overhead and unpredictability and it will diminish the proficiency of the old steering protocol.RSA calculation and symmetric encryption utilizes DES calculation.

U-prove based security framework for mobile Device authentication in ehealth networks by Khan Zeb, Kashif Saleem, Jalal Al Muhtadi, Christoph Thuemmler in 2016. Proposed an Individualized Medicine/Precision Medicine are intended to improve nature of experience, diminish conditions and discharge productivity holds, particularly with regards to the (self)- administration of incessant, non-transmittable sickness. In disconnected mode to get ongoing information specifically from the embedded gadgets and additionally eHealth pack. Relatively more adaptable and does not require cell phones inserted equipment security include for qualification sharing counteractive action and security. The most straightforward, effective and broadly utilized mysterious property based certifications (ABC) innovations in people in general key framework (PKI). Various difficulties are confronted with respect to human services including the ascent of endless, non-transferable ailments, steadily expanding medicinal services expenses, and maturing social orders. The issuance convention, the token is created by consolidating the guarantor's open key with the client's qualities. The safe eHealth application on cell phone won't login to build up secure channel with server for correspondence. On the off chance that the inquiry does not execute, the entire procedure is dropped and server backpedals into the tune in and acknowledge mode. U-Prove innovation based security structure.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

A layered and componentized security architecture for linux based mobile network Elements by shanghua zhang, aixin zhang, jun wu, longhua guo, jiahua li, bei pei in 2015. Proposed the interface that is given by the nearby lower layer. For whatever length of time that the interface of this layer and the interface of the nearby lower layer is characterized, the engineers can concentrate on the capacities and strategies utilized as a part of the improvement of a layer. The request transforms, it is anything but difficult to utilize the new security module rather than the first segments. The security design in light of parts can lessen the reliance between the frameworks. High versatility, high compactness, and totally free elements. Furthermore, it can accomplish the impact of high union and low coupling. Enhance the execution of Linux framework and diminish the work weight of designer and convention to enhance the wellbeing execution of Linux framework. The DAC most serious issues is the subject specialist is too enormous. It might uncover data coincidentally. DAC is a sort of successful approaches to shield the framework assets from unlawful get to. Organize components confront genuine security dangers and security dangers to battle against expanding digital assaults. The versatile system has open, heterogeneity, portability and element attributes, arrange components confront a genuine security danger and security dangers. The Linux part has not given a general base support for these get to control models and structures. Symmetric encryption calculation, HASH calculation, hilter kilter encryption calculation and personality verification, encryption transmission.

III. MOBILE SECURITY THREATS

Forecast of mobile security trends and vulnerabilities that concern us most. Threats is not to raise alarm or panic, but to paint a picture of the gravest security concerns we face in the coming year, and hopefully, encourage the industry at large to prepare for them now. With the proper precautions, most of them can be minimized, or forestalled altogether.

I. Terrorism

The horrific attacks in Paris, San Bernardino, and other locales around the world ensure that terrorism will overshadow mobile security concerns next year. We will see growing concern over usage of Telegram and Redphone-type communication apps that use end-to-end encryption to avoid eavesdropping. Tracking the appearance of legitimate-looking apps that criminals are using to communicate with each other for a very temporary time period (sometimes only once).

II. Hackers Target Mobile Payment Services

Based on back channel murmurs among black hat hackers, it's more likely than not that leading mobile payment platforms such as Apple Pay or Samsung Pay will be seriously compromised in 2016. This will probably happen not through outright breaking of their payment processing algorithms but via analysis of the entire system to identify bypass measures and vulnerabilities, leading to credit card information fraud, extortion, and unauthorized use. We have already know how stolen credit card infomation has been successfully added to ApplePay accounts without bank verification, allowing fraudsters to use stolen card information at brick-and-mortar stores. Soon, a similar technique will likely be used for online transactions. Peer-to-peer mobile payment apps such as Venmo that use simple payment remittance processes will become more vulnerable to hackers attempting to transfer funds from users' accounts to dummy accounts they can then access.

III. The Rise of Mobile Web Browser-Based Hacking

We expect mobile versions of Chrome, Firefox, Safari, and related kernels on Android and iPhone to be hacked frequently in coming months. Hacking via a mobile browser is one of the most efficient ways to compromise the entire phone, because exploiting a browser vulnerability can enable the hacker to bypass its many system-level security measures. The following will gives a sense of how this would work:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 20, April 2026 Impact Factor: 8.2

• Webkit-based exploits allow hackers to bypass a browser's sandbox, or the security measures built into modern browsers. This would most likely be followed by OS/kernel-level exploits to access the root of the system and gain total control over the device.
• An example OS-level exploit is Stagefright, which was a weakness in a library inside the Android OS. Although Google released a patch to address this problem over the summer, Zimperium released a second set of vulnerability discoveries, dubbed Stagefright 2,0, in October. When such an exploit is executed via a web-browser, it becomes extremely reliable.

IV. Remote Device Hijacking/Eavesdropping

The explosive growth of Android devices, billions of people around the world will soon own a smart phone. Most of these handsets include preloaded applications that are generally not analyzed or validated by Google's security team, exposing them to remote device hijacking. Related to this is the rising threat of man in the middle attacks (or MitM). New smart phone owners are often not aware of or practicing adequate security habits with their device. For instance, they may allow their device to automatically access unsecured AP/WiFi connections that don't encrypt data communicated through the network. This can lead to insecure apps leaking user credentials, which hackers can "see" when the mobile device transmits data.

V. DDoS Attacks: Evolved

Up to now, most Denial of Service attacks have been an infrequent and short-lived annoyance, one that most businesses online are relatively well-equipped to deal with. However, the growth of mobile and other Internet-connected devices is allowing the DDoS to evolve. We are starting to see devices hijacked and turned into DDoS bots, thereby increasing the barrier to detect and prevent denial of service attempts. We should prepare for many such attacks, roughly growing at the rate in which new Internet-connected devices enter the market.

VI. The Internet of (Vulnerable) Things

The recent hacking of children's wireless toys, not to mention the hacking of an automated car, highlights the dangers. More and more devices are becoming Internet-enabled but without proper security configurations/measures, providing for an increased attack surface and more variables to go wrong among the proliferating operating systems, drivers, and software that run them. All mobile apps that connect to IOT devices through Bluetooth or Wi-Fi are vulnerable, and accessing a private, secure network. Internet-connected medical devices are notorious for having poor configurations from a security standpoint, allowing hackers to access and gain remote control of them. For instance, networked ultrasound scanners and other medical devices often have a hardcoded default login/password for remote login that is relative easy to guess.

V. SECURITY ISSUES METHODS TO SOLVE:

Mobile devices face an array of threats that take advantage of numerous vulnerabilities commonly found in such devices. These vulnerabilities can be the result of poor technical controls, but they can also result from the poor security practices of consumers. The GAO states "Private [companies] and relevant federal agencies have taken steps to improve the security of mobile devices.
The GAO report gives a list of mobile vulnerabilities ,which are common to all mobile platforms.
• Mobile devices do not have passwords enabled. Mobile devices lack passwords to authenticate users and control access to data stored on the devices. Many devices have the technical capability to support passwords, personal identification numbers (PIN), or pattern screen locks for authentication. Some of mobile devices also include a biometric reader to scan a fingerprint for authentication.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 20, April 2026 Impact Factor: 8.2

• Two-factor authentication is not always used to conducting sensitive transactions on mobile devices. Consumers generally use static passwords instead of two-factor authentication when conducting online sensitive transactions while using mobile devices.

Static passwords for authentication has security drawbacks:

passwords can be guessed, forgotten, written down and stolen. Two-factor authentication generally provides a higher level of security than traditional passwords and PINs, and this higher level may be important for sensitive transactions. Mobile devices can be used as a second factor in some two-factor authentication schemes. Without two-factor authentication, increased risk exists that unauthorized users gain access to sensitive information and misuse mobile devices.

• Wireless transmissions are not always encrypted. Information such as e-mails sent by a mobile device are usually not encrypted while in transit. When a wireless transmission is not encrypted, data can be easily intercepted.

• Mobile devices may contain malware. Consumers may download applications that contain malware. An application could be repackaged with malware and a consumer by mistake download it onto a mobile device, the data can be easily intercepted.

• Software on the mobile devices may be out-of-date. Security patches for third-party applications are not always developed but released in a timely manner. Unlike traditional web browsers, mobile browsers rarely get updates. Using outdated software increases the risk that an attacker may exploit vulnerabilities associated with these devices.

• Mobile devices often do not have limit Internet connections. A firewall secures these ports and allows the user to choose what connections he wants to allow into the mobile device. Without a firewall, the mobile device may be open to intrusion through an unsecured communications port, and an burglar may be able to obtain sensitive information on the device and misuse it.

• Communication channels are poorly secured. Communication channels, such as Bluetooth communications, open or discovery mode could allow an attacker to install malware through that connection. Using unsecured public wireless Internet networks or WiFi spots could allow an attacker to connect the device and view sensitive information.

The following new ideas are included for mobile security:

• Enable user authentication.
• Enable two-factor authentication for sensitive transactions.
• Verify the authenticity of downloaded applications.
• Install antimalware capability.
• Install a firewall.
• Install security updates.
• Remotely disable lost or stolen devices.
• Enable encryption for data stored on device or memory card.
• Enable white listing : White listing is a software control that permits only known safe applications to execute commands.
• Establish a mobile device security policy.
• Provide mobile device security training.
• Establish a deployment plan.
• Perform risk assessments.
• Perform configuration control and management.

VI. CONCLUSION

We discussed security and safeguard are vital parts in system administration framework. Also an attack in MANET is exceptionally helpless for every one of the layers and the SRA(Smartphone Risk Assessment) is thought to be useful for clients to decide potential dangers of their cell phones and any applications that can possibly release delicate information. It is believable that a customer's rightful demand from one area might be denied at another area. It is a

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 20, April 2026
Impact Factor: 8.2

novel approach in 1M(Instant manager) authentication technique to lift the security level of information. There are distinct lack of literature regarding mobile security. The number of articles written has risen significantly, but not rise in mobile smartphone usage worldwide. Atlast, there are no clear solutions presented to the Mobile Security issues, which leaves an area for future scholarly research.

REFERENCES

1. Hu, Jiankun, et al. "Biometric security for mobile computing." Security and Communication Networks 4.5 (2011): 483-486..
2. N. Mallat, "Exploring consumer adoption of mobile payment - A qualitative study," The Journal of Strategic Information Systems, vol. 16, no. 4, pp. 413-432, Decmeber 2007.
3. M. Finneran, "Mobile security gaps abound," InformationWeek, vol. 1333, pp. 26-29, 2012.
4. [4]P. Barford, J. Kline, and D. Plonka, "A Signal Analysis of Network Traffic Anomalies," Proceedings of ACM SIGCOMM Internet Measurement Workshop, pp.71–82, Marseilles France, 2002.
5. M. Roughan, T. Griffin, M. Mao, A. Greenberg, and B.Freeman, "Combining Routing and Traffic Data for Detection of IP Forwarding Anomalies", ACM SIGMETRICS Performance Evaluation Review, 32(1), pp.416–417, 2004.
6. T. Blitz, "Decoding mobile device security," Security, vol. 5, no. 42, pp. 46-47, 2005.
7. G. Hurlburt, J. Voas and K. W. Miller, "Mobile-app addiction: Threat to security?," IT Professional Magazine, vol. 6, no. 13, pp. 9-11, 2011.
8. MS. Kim, HJ. Kang, CS. Hong, HS. Chung, and JW. Hong, "A Flow-Based Method for Abnormal Network Traffic Detection", Proceedings of the IEEE/IFIP Network Operations and Management Symposium, pp.599–612 Seoul, Korea, 2004.
9. Hezal Lopes et al. Int. Journal of Engineering Research and Application www.ijera.com Vol. 3, Issue 5, Sep-Oct 2013, pp.499-502