iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IX **Month of publication:** September 2022

DOI: https://doi.org/10.22214/ijraset.2022.46703

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IX Sep 2022- Available at www.ijraset.com

Literature Review of Mobile Security Enhancement

Rakesh Kumar[1], Dr. Anant Kumar Sinha[2], Dr. Narendra Kumar[3], Arif Md. Sattar[4]
[1]*Research Scholar, M. U. Bodh-Gaya*
[2]*Associate Prof & Head, Dept. of Physics, A. M. College, Gaya.*
[3, 4]*Assistant Prof., Dept. of Computer Applications and IT, A. M. College, Gaya*

Abstract: ***The presented article provides an overview of related literature on the subject of mobile security. The issue was selected as a result of the increase in mobile applications and the underdeveloped discussion surrounding the security of those applications. Cell phones and tablets with mobile operating systems are regarded as mobile devices for the purposes of this essay. More specifically, these are BlackBerry OS (RIM)., iOS, and Android from Google, respectively Even though it's crucial to understand these concepts, the security flaws in the Android OS are the main subject of this literature review. Malware that changes to be somewhat different from the previous version is referred to as polymorphic. Although the malware's functioning is unaffected by the automated code changes, they may make traditional anti-virus detection technologies ineffectual.***
The method used to target a certain technology is the simplest way to define an attack vector (i.e. a path used to compromise a particular system). A group of "zombies" that are remotely managed for harmful or financial purposes makes up a botnet. Many times, a single botnet consists of hundreds or even thousands of devices. When the word "vulnerability" is used in this document, it refers to a weak point that makes a system's security more susceptible to attack. When three factors—a system weakness or flaw, attacker access to the weakness, and attacker capability to exploit the weakness—intersect, a vulnerability results.
Keywords: Mobile Security, Smart Phone, Malware Attacks, Botnets, Android, IOS, Polymorphic

I. INTRODUCTION

As organizations start to rely on these devices for routine tasks, the need for mobile device security has increased. However, it has been determined that these gadgets have no security. Only 10% of the 86 million gadgets in use today, on average, are protected. The news has increasingly focused on the hot button issue of how to secure these mobile devices for both personal and professional use, but there has been little to no research on how to do so. As the number of Android devices has increased significantly over the past few years, Android security has received considerable attention. Device activations have increased by 250% just in the past year, and Google's "Play" market has seen more than 11 billion app downloads and still counting.
Android and iOS are the two most widely used mobile operating systems. Similar to how different iOS versions include iOS 13, iOS 12, iOS 10, etc., different Android operating systems include Nougat, Lollipop, and Marshmallow. Only 11% of Android mobile users have the most recent Android operating system, compared to 86% of iOS users. According to the Open Web Application Security Project's analysis of mobile hazards, insecure data storage and insecure communication risks are the most serious issues with mobile security. This paper outlines some key mobile device security issues and suggests some preventative measures.

II. SECURITY ATTACKS ON MOBILE

Day by day the security attacks on mobile devices are increasing and most of them are insecure data storage and communication. Some of the critical and conspicuous mobile attacks are summarized below:

1) *Security of Data Storage:* Many mobile applications use weak cryptographic techniques, and 87.7% of mobile apps save data in plain text format. If a mobile device is taken from its owner or lost, the person who finds it has access to all of the personal and confidential data on it. By enticing the user to install a mobile application that is infested with malware, data can also be stolen from mobile devices.
2) *Security During Communication:* The majority of communications used a client-server approach on mobile devices. Applications on mobile devices take on the role of a client and communicate with their servers to store various kinds of user data. The developer must set up secure communication between their server and their mobile application. Sniffing tools have made it simple for an attacker to intercept communications between a mobile device and a public Wi-Fi hotspot. The attacker can take important data from the user if the used connections are not secure. If the developer uses a weak SSL configuration for communication with the app server, phishing and Man-In-The-Middle (MITM) attacks can be launched.

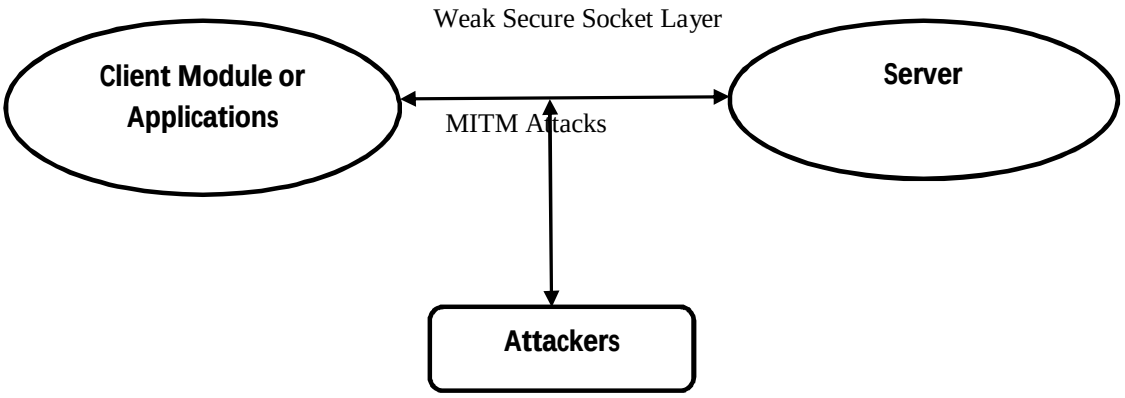


Figure 1: Weak SSL Mobile Communication

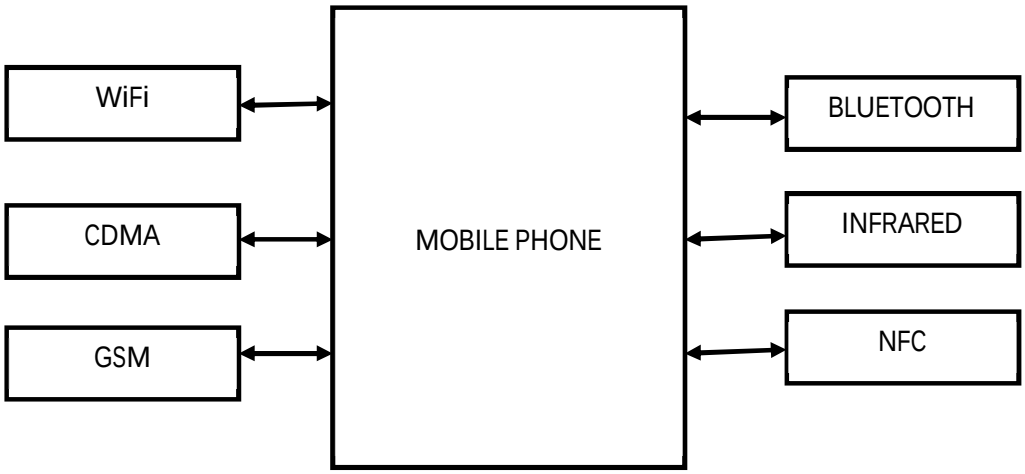


Figure 2: Various Techniques Used in Mobile Communication

3) *Security from Cross Site Scripting Attacks:* One type of serious online application attack is cross-site scripting (XSS) assault. Many developers employ HTML and JavaScript to build hybrid mobile applications; nevertheless, these hybrid mobile applications' insecure code makes them vulnerable to XSS assaults on mobile devices. An attacker can modify the behavior of the mobile device using these vulnerabilities. Sharing is a popular pastime on mobile devices, and an attacker can distribute a link to a malicious software from a reputable website by taking advantage of an XSS vulnerability there.
4) *Security from Malware Attacks:* Without the user's awareness, malware or dangerous software is installed on their mobile device. Malware can propagate via insecure applications or the internet. Malware has the ability to collect and communicate sensitive information to attackers, giving them complete control of the mobile device. It can send messages to the entire contact list or to undesirable numbers.

Below is a list of the various categories of the most prevalent mobile malware.

a) *Worms:* Mobile worms replicate themselves and spread to other mobile devices in a manner similar to traditional computer worms. Without user engagement, mobile worms can propagate via SMS or other communication channels.
b) *Trojan:* When a user runs the trusted executable files that contain the harmful instructions (Trojan), the Trojan is triggered. Trojan can be used to steal data, disable some mobile device features, and allow an attacker to install other malware.
c) *Spyware:* The main goal of spyware is to steal and spread users' sensitive or personal information without their awareness.
d) *Ghost Push:* After gaining root access to a mobile device, this malware downloads malicious apps, changes them to system apps, and then loses root access permissions. Users may need to perform a factory reset on their mobile devices to get rid of these infections. This kind of malware can rob users of their private data.

III. LITERATURE REVIEW

1) N. Leavitt (2011), suggested that there are two primary attack vectors for mobile phones. The first is when a mobile phone connects the internet; the second is when a mobile phone connects to a network. Because to much individual and financial data is being stored on a phone, this is making the mobile phone environment more and more appealing to hackers. 2010 saw a 46% boost in mobile phone security, according to McAfee Labs, and every day, more than fifty five thousands (55,000) new mobile malware variants are discovered there [1]. While PCs are increasingly being used to establish mobile botnets, the main goal of mobile malware is to steal money and personal information. Similar to the emergence of android botnets, this issue has been a topic of discussion for the past year [2]. Due to the mobile nature of smart-phones, the aforementioned blogger, Marko, properly compares the concept of an Android botnet to a salesman who is on the road and infected with tuberculosis.
2) Mario Ballano (2011) , a Symantec researcher, claimed to have discovered a new attack method for Android that is comparable to Windows DLL hijacking [3]. This is more of a vulnerability in some apps that dynamically load code utilizing the Android classes Public Constructors and DexClassLoader than it is an OS flaw. Ballano claimed that the few apps that he found to be susceptible to this technique have been reported to Google. As of November 2012, Google's response to the issue is unknown, and a patch has not yet been released. Another attack method for Android phones is fake online "Google Play" stores. Tim Wyatt, a software engineer at Lookout, informs us that GGtracker Trojan-infected software distributed through fake online shops has the ability to sign up users for premium SMS services without their consent or even informing them that a transaction has taken place.
3) Khan et al. (2015) researched several security-related difficulties, risks, and vulnerabilities for mobile users [4]. Their analysis includes a number of different mobile dangers, including physical threats, application-based threats, network-based threats, and web-based threats. One issue involving earnest money and mobile weaknesses is a botnet. They claim that biometric authentication is a key security defense mechanism for mobile security and data privacy. Every phase of developing a mobile application must include security mechanisms.
4) Cifuentes et al.(2015) conducted an analysis of the flaws discovered in health-related mobile applications [5]. In order to identify vulnerabilities, they divided mobile health apps into six groups depending on the functionalities of the apps and downloaded 10 Android apps from the Google Play store for each group. 60 m-Health apps have 157 vulnerabilities in total. According to their findings, the majority of vulnerabilities and high-risk levels are present in apps with remote monitoring capabilities. Their findings indicate that 64% of the flaws in m-Health apps linked to unreliable input.
5) Chatzikonstantinou et al.(2016), revealed cryptographic vulnerabilities in mobile applications and categorized as fragile cryptographic algorithms, weak cryptographic keys, and feeble implementation of cryptographic methods, and weak parameters [6]. They manually conducted static and dynamic analyses on 49 arbitrary Android apps that they downloaded from the Google Play store. According to their findings, 12.2% of Android apps have no cryptographic methods at all, while nearly 87.8% of Android apps use weak cryptographic algorithms.
6) Shukla et al. (2015) A new key concord and authentication procedure for Electronic Health Record systems was put into place[7]. Since the EHR system has a variety of users, including doctors, lab workers, patients, and insurance agencies, adequate key agreements and authentication are essential. The suggested protocol operates on a commitment system and will halt communication if authentication is unsuccessful. They claimed that the binding/hiding aspect of the protocol makes Man in the Middle attacks particularly difficult to execute in wireless communications.
7) According to Choo (2014), advancements in new technology and advancements in security measures must happen simultaneously [8]. According to the routine activity idea, criminal activity happens when there is a motivated attacker, a targeted gadget, and a weak guardianship. The ability of cloud storage applications like DropBox, Google Drive, One Drive, etc. to hold a sizable amount of user data makes them popular targets for attackers. They looked at celebrity iCloud accounts that had been compromised and found that the majority of hacks target specific security questions, usernames, and passwords.
8) According to Agasi (2015), there isn't a perfect way to prevent issues with mobile security. Implementing appropriate security rules, incorporating current security, and protecting data on mobile devices are the key concerns with mobile security [9]. Corporates must build a secure environment for mobile devices, threat management, and security rules that are independent of the devices and operating systems used in them in order to secure company documents and data.
9) Cheng et al. (2007) proposed a virus detection and alert system for smart-phones. by. It identifies viruses by gathering activity data from the smart phones and doing joint analysis to identify odd behaviors on both a single device and the entire system. When a potential infection is identified, they employ a proxy to offload the processing load from resource-constrained smart-phones, and the proxy delivers targeted alerts to infected devices and a fraction of the uninfected devices to stop the spread. The

scientists asserted that the approach can successfully stop widespread viral outbreaks while requiring minimal overhead. In order to improve security perception, this study offers a useful mobile technology-based learning approach that puts the needs of the students first. The strategy outlines the creation of a modular mobile security software that addresses both established and new security concerns and threats. This strategy offers students a practical and efficient way to improve the security of their devices as using smart devices is increasingly becoming a part of their daily routines.

10) Ruitenbeek et al. (2007) conducted a research on the spread of smart-phone viruses, focusing in particular on the consequences of multimedia messaging system (MMS) viruses that proliferate by sending infected messages to other devices, and they put forth a number of response mechanisms to gauge the efficacy of virus mitigation techniques. In their paper, the authors present a virus model that "parameterized and represented a wide range of potential MMS virus behaviors and identified four MMS virus scenarios." In each scenario, the residing virus on the phone manages to send MMS messages with an attachment file of infecting capacity to other phones that are chosen from its contact list as well as dialing a random phone number.

When a user opens an infected attachment file, a virus is installed, infecting the target phone and putting it under the attacker's control. For each of the four scenarios, the following reaction mechanisms have been evaluated:

a) Scanning all MMS attachments at MMS gateways for viruses detection;
b) Promoting user education to increase user awareness;
c) Immunizing devices with software patches;
d) Keeping an eye out for unusual behavior; and
e) Creating a blacklist of suspected infected phones

The outcomes of their experiments demonstrated that any reaction mechanism must be swift enough to react quickly to viruses that are propagating. Although the authors' work is quite persuasive, they stated that an ideal virus response strategy must be able to address a variety of virus behavior and that their work may be improved upon by evaluation extensions.

The aforementioned Android Security concerns don't have any obvious answers. All cryptology (or information security protection) relies on two elements: something you know while something you possess. The ideal representations of this circumstance are an access card and a password. Many times, only one of these things is required, and occasionally, in the most secure locations, both are required. The demand for a quick but reliable biometric solution has increased dramatically since mobile computing has turned into a repository for all personal things including bank accounts, email addresses, and phone numbers. Additionally, malware detection services now have a larger battery consumption than the majority of programmes, which forces consumers to turn off any previous security measures. Users are more inclined to leave these security services on if malware prevention was more battery-efficient and energy conscious.

In the PC industry, polymorphic malware has a notorious reputation, and it seems like new malware detection and prevention techniques are created every month. Polymorphic malware classification is a persistent, continuous challenge. As new techniques are created to combat polymorphic malware, fresh concepts are generated on how to defeat the new detection techniques.

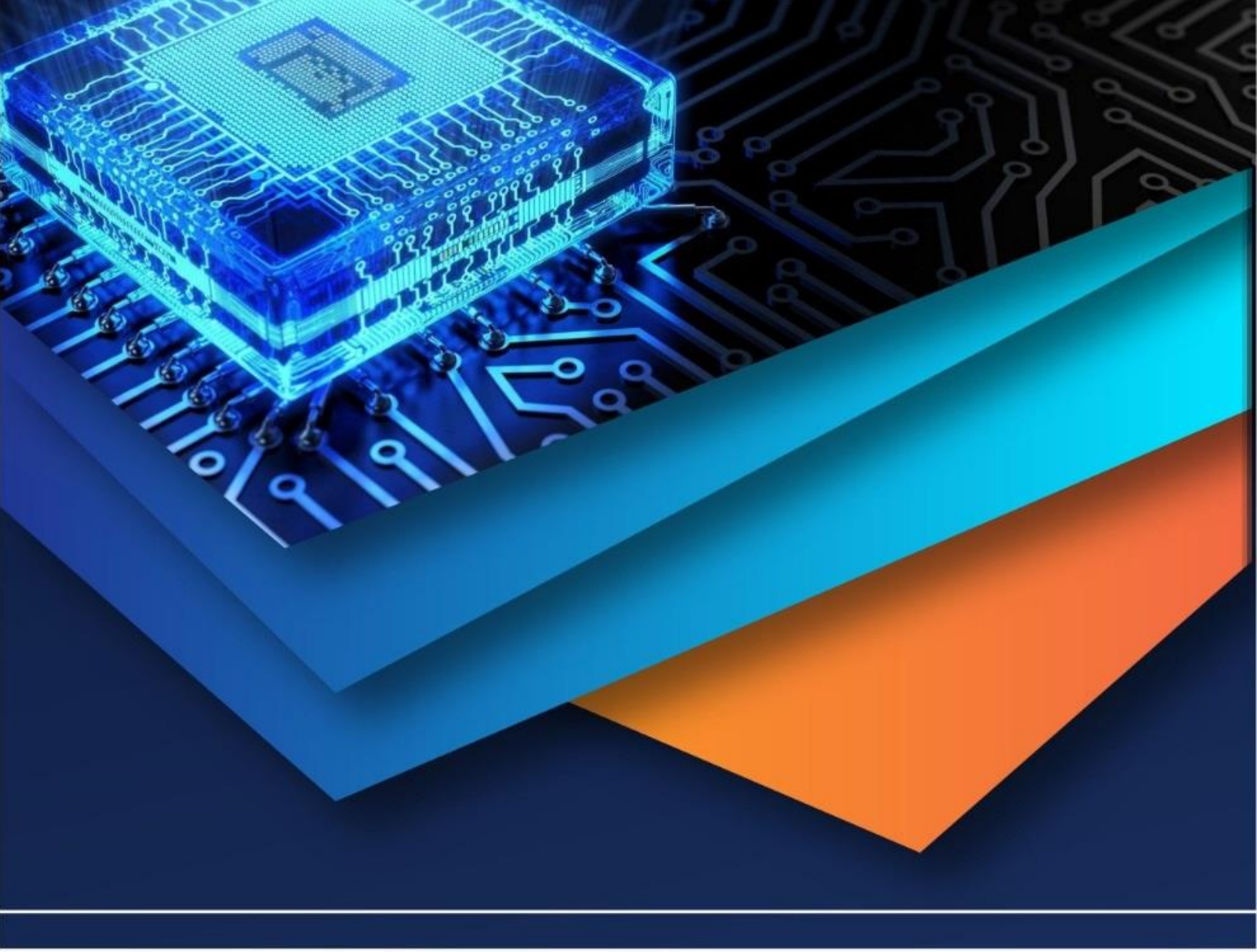
IV. CONCLUSION

Particularly when it comes to polymorphic and botnet security, there seems to be a notable dearth of material on Android security. The amount of articles written has greatly increased, although not by as much as may be anticipated given the increase in mobile smart-phone usage globally. Last but not least, the Android Security problems are not clearly addressed, leaving room for further scientific investigation. of malware attacks. Security tool manufacturers concur that it is very challenging to safeguard the complete spectrum of goods because risks are dispersed and not concentrated in one area. They suggest a few standard precautions to guard against security lapses. There is need of intense research pertaining to security of mobile storage and communication.

REFERENCES

[1] N. Leavitt, "Mobile security: Finally a serious problem," Computer, vol. 6, no. 44, pp. 10-15, 2011.
[2] K. Marko, "Rise of android botnets.," Informationweek - Online, 2011.
[3] "More mobile security glitches," Computer Fraud & Security, no. 7, p. 3-4 , 2011.
[4] Khan, J., Abbas, H., & Al-Muhtadi, J. (2015). Survey on Mobile User's Data Privacy Threats and Defense Mechanisms. Procedia Computer Science, 56, 376-383.
[5] Cifuentes, Y., Beltrán, L., & Ramírez, L. (2015, August). Analysis of Security Vulnerabilities for Mobile Health Applications. In 2015 Seventh International Conference on Mobile Computing and Networking (ICMCN 2015).

[6] Chatzikonstantinou, A., Ntantogian, C., Karopoulos, G., & Xenakis, C. (2016, May). Evaluation of Cryptography Usage in Android Applications. In proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies, pp. 84-91.
[7] Shukla, V., Chaturvedi, A., & Srivastava, N. (2015). A new secure authenticated key agreement scheme for wireless (mobile) communication in an EHR system using cryptography. Communication on applied electronics (CAE), 3(3), pp. 17-22.
[8] Choo, K. K. R. (2014). Mobile cloud storage users. IEEE Cloud Computing, 1(3), 20-23.
[9] Agasi, O. (2015). Encapsulating mobile security. Computer Fraud & Security, 2015(6), 10-12.
[10] Cheng, J., Wong, S. H., Yang, H., & Lu, S. (2007)"Smart-siren: virus detection and alert for smart-phones", In Proceedings of the 5th international conference on Mobile systems, applications and services, pp. 256-61.
[11] Van Ruitenbeek, E., Courtney, T., Sanders, W. H., & Stevens, F. (2007). Quantifying the effectiveness of mobile phone virus response mechanisms. pp. 790-800, In 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY