IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 2, Ser. III (Mar - Apr 2019), PP 49-52
www.iosrjournals.org

Proposing Mobile Based Secured Remote control, sharing, data transfer and web conferencing software tool

Shubhangi Jena[1], Varun Nair[2], Arrvind Sethuraman[3], Chinmay Raut[4]
[1]*B.E Student Dept. of Computer Engineering UCoE, Mumbai, India*
[2]*B.E Student Dept. of Computer Engineering UCoE, Mumbai, India*
[3]*B.E Student Dept. of Computer Engineering UCoE, Mumbai, India*
[4]*Assistant Prof. Dept.of Computer Engineering UCoE, Mumbai, India*
Corresponding Author: Shubhangi Jena

Abstract: *Remote desktop controlling provides remote support, remote access and online meeting software that the world relies on. This paper emphasis on providing seamless higher security for remote control devices for website conference, troubleshooting and desktopsharing. The paper presents a remote-desktop based on remote debugging model for the situation that hardware programming experiment is not often conducted in the network innovation experiment and teaching. One of the remote desktop utility Team Viewer is used as a stepping stone in order to achieve more secured remote control.*
However there were security concerns regarding this application and users felt that it would not provide an appropriate solution to their security flaws. Providing more security to remote control data transfer has been proposed in this paper. Steps to achieve more security has to the application has been introduced in this paper.
Keywords: *Security; remote control; innovation; troubleshooting; desktop sharing.*

Date of Submission: 29-03-2019 Date of acceptance: 13-04-2019

I. Introduction

Desktop-to-Desktop access is common. A novel idea to allow the accessibility for mobile-to-desktop. The main concern is network security.Networkprevent and monitor unauthorized access, misuse, modification, or denial of a computer networks and network-accessible resources. Only Network security can protect you from Trojan horse viruses. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. The main aim of this paper is to solve the security issues that come into picture when people try to connect mobile-to-desktop or desktop-to-desktop.

Remote Desktop Utility tool enables users to gain access to a desktop remotely (as the name suggests) and troubleshoot as well. Quite widely used software/tool also enable features such as file sharing and online calls. Due to additional feature, increasingly more number of users flock to one tool for accessing the various features.

However, witnessing the rise of security threats in widely accessed remote desktop utility tool, the paper focuses on the history, timeline of developments and threats/attacks and a novel idea to thwart similar attacks which otherwise spelled in a mass 'digital heist' of private data.

Ultimately, the paper also articulates a solution to address the inefficiency of the existing security layers to provide an enhanced robust system to all users.

II. Literature Review

In citation [1] Varun Nair discusses all the Security evaluations and shortcomings of the Team Viewer software the author uses a grading system to help us understand the quality of the product that he emphasis on the various grading points which are there and then he attempts to comprehend the quality of the project.

Varun Nair tries to comprehend the technology in citation [2] that has used and the various protocols that has been implemented for the desired outcome of the current and existing project and architecture of the proposed system that is going to be designed

The process of citation [3] tends to explainAndroid based lab control is a system which allows you to access desktop of remote computers. The reference explains how he designed his project what all methods and protocols were used in the making and he has introduced a new concept in this project.

Through citation [7] co-author Shubhangi Jena throws light on the security threat faced by the large community of the widely used remote desktop utility tool 'TeamViewer'. The suspicion around a hack gathered upheaval in the community after unauthorized connections had been reported.

In citation [9], co-author Arrvind Sethuraman discusses another security threat wherein a ransomware had been installed stealthily in the user's desktop and which operated through memory. The point proved here is the inefficiency of the current security layers of TeamViewer application and how users data is always at stake.

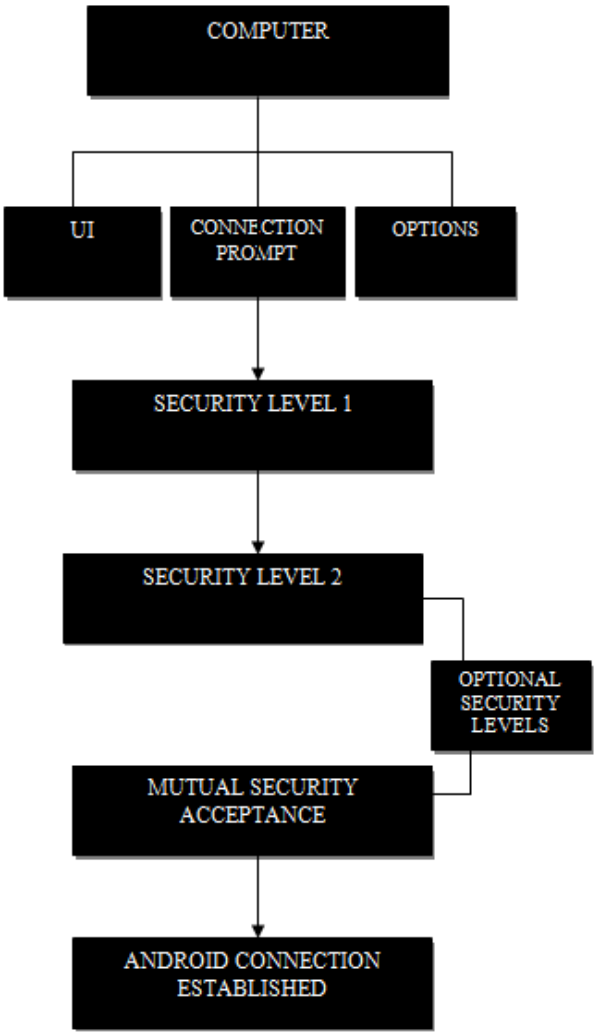

Fig 1.1 Illustration of step by step procedure of heightened security measures in a remote desktop access utility tool.

III. Proposed System

The idea proposed is very stimulating and comprehensive. The idea is to provide more security to data transfers using certain steps which will be unique for a certain connection made between two remote users. The aim is not only to provide better security but also better user interface

The users can choose multiple security configurations to enhance their experience where two level security is mandatory. The algorithm proposes to quickly circulate the entire cycle of process

Furthermore, At first the user should pre-define what their security measure should look like and then use that security setting as their measure to begin their remote control connection. This would not only maintain the confidentiality level but it would also improve existing system. The keywords would not remain in the server and would get disposed as soon as the session closes from the users activity scenario.

Data in this proposed application is typically balanced and approaches to reduce the amount of time the data stored in the server to a constrained duration. A new methodology is placed so as to maintain the efficiency between the user interface and the system for deployment. At first the application is installed into the personal computer and the the respective source code is applied to the cellular device.

The first process is to register the user with the personal computer and the mobile and proceed by logging in with ,respective username and password which is the first level security; Here the user can change the settings to increase the level of security and choosing what kind of security level should be carried on with in the future sessions

After the procedure for which has been completed, the connection between computer and the cellular device has been established

Lastly after the user has been logged out, the password generated would be reset and new password would be generated the next time the user logs in.

The algorithm which would be implemented is a new algorithm to maintain mutual understanding between the programming module called a DS2-511

DS2-511 ALGORITHM

STEP 1- **INPUT** USERID AND PASSWORD

STEP 2- IF ACCEPTED GOTO STEP 5

STEP 3 – ELSE GOTO STEP 2

STEP 4 – **INPUT** SECURITY LEVEL

STEP 5 – IF SECURITY LEVEL= USER THENGOTO STEP 6 ELSE GOTO STEP 4

STEP 6 – **START** CELLULAR DEVICE WHERE SECURITY PROTOCOL = CELLULAR DEVICE

STEP 7 – IF SUCCESS GOTO STEP 9

STEP 8 – ELSE GOTO STEP 6 OR STEP 5

STEP 9– STOP

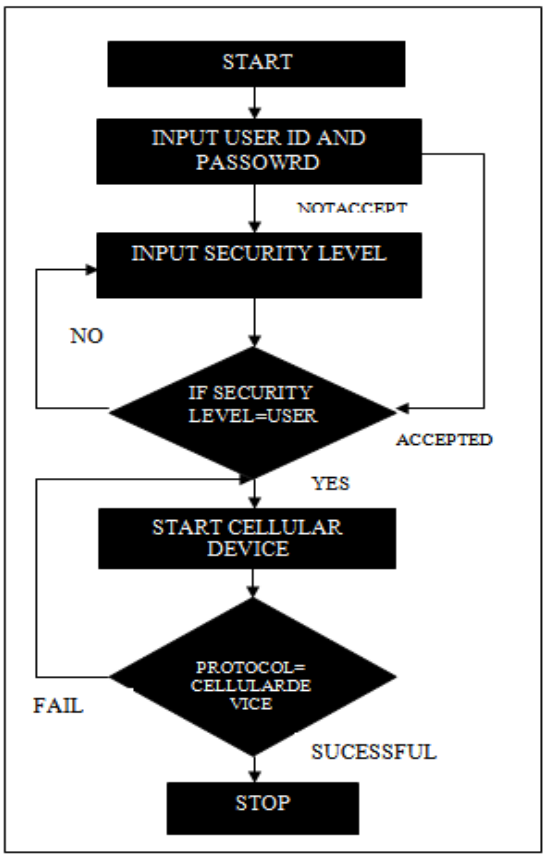

Fig. 1.2 Flowchart depicting the steps for enhanced security

IV. Future Works

Although, there are various advanced projects or products implemented.The main goal of this proposed project is to give rise to enhanced security measures so that the users and authorized personals can totally be dependent on the structured data that would be flowing within the relationship between the software and hardware. The proposed model should not only give out multiple future scopes but also should know how to bridge the gap between the past, present and future advancements of this implemented project, As the amount of data that has been collected and stored needs to be refurbished.

V. Conclusion

With the advent of 5th generation around the corner the speed for remote control devices would not only done systematically but also seamlessly so as to provide better environment between the user and the software. This eliminates the risks of bugs encountered and adds much more efficient hodgepodge of security, interaction and work that needs to be done systematically.With enhanced security, more traffic will be generated for this remote desktop utility tool and there would be improved privacy as well as no security breach and hence there would be proper encrypted data transfer with the amount of data that has been garnered. Lastly this would also give rise to productivity and better computing software.

References

[1]. STJEPAN GROŠ "SECURITY RISK ASSESSMENT OF TEAMVIEWER APPLICATION"PROCEEDINGS OF THE ITI 2011, 33RD INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY INTERFACES 04 AUGUST 2011″

[2]. Implementation of Remote Desktop UtilityJournalVirtual Lab Control Using Android Phone – Journal

[3]. Swati Khandelwal.New TeamViewer Hack Could Allow Clients to Hijack Viewers' Computer. Available: https://thehackernews.com/2017/12/teamviewer-hacking-tool.html

[4]. Security risk assessment of TeamViewer application - IEEE Conference Publication. Available: https://ieeexplore.ieee.org/document/5974003/authors

[5]. Suhashini Chaurasia," Implementation of Remote Desktop Utility using Teamviewer" IOSR Journal of Computer Engineering (IOSR-JCE), (NCRTCSIT-2016).

[6]. Mayur Jagtap, Suryakant Nachan, Vandana Nagre, Snehal Shivathare" Virtual Lab Control Using Android Phone" International Journal of Scientific and Research Publications, Volume 5, Issue 3, March 2015.

[7]. "Hack Suspected on TeamViewer After Users Report Unauthorized Connections". *Trend Micro*. Retrieved 2016-06-03.

[8]. "TeamViewer denies hack after PCs hijacked, PayPal accounts drained". The Register. UK. Retrieved 2016-06-03.

[9]. "Surprise Ransomware Installed via TeamViewer and Executes from Memory". *Bleeping Computer*. Retrieved 2016-03-23.

[10]. Santosh Dahifale, Ritukumari Pandey, Rahul Ballani, Sagar Ingle. "Android Desktop Control (ADC)". International Journal of Scientific and Technology Research Volume 3,Issue 4,April 2014

[11]. Angel Gonzalez Villan, Josep Jorba Esteve" Remote Control of Mobile Devices in Android Platform" IEEE TRANSACTIONS ON MOBILE COMPUTING

[12]. Tristan Richardson, Quentin StaffordFraser,Kenneth R. Wood and Andy Hopper,Reprint "Virtual Network Computing" IEEE Internet Computing Volume 2, Number 1 January/February 1998.

[13]. A. P. Rajshekhar, Socket Programming in Java

[14]. Jaya Bharathi chintalapati1, Srinivasa Rao T.Y.S. "Remote computer access through Android mobiles." IJCSI International Journal of Computer Science Issues, September 2012.

[15]. Muhammad Wannous, Student Member, Hiroshi Nakano, "NVLab, a Networking Virtual Web-Based Laboratory that Implements Virtualization and Virtual Network " Computing Technologies IEEE.

[16]. Dixit, S.,"Data rides high on high-speed remote access",Communications Magazine, Volume: 37, Issue: 1,Jan 1999

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Shubhangi Jena. " Proposing Mobile Based Secured Remote control, sharing, data transfer and web conferencing software tool" IOSR Journal of Computer Engineering (IOSR-JCE) 21.2 (2019): 49-52.