Journal of Information Security, 2019, 10, 250-262
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Improved Smartphone Application for Remote Access by Network Administrators

Ekwonwune Emmanuel Nwabueze[1], Etim Emmanuel Okon[2]

[1]Department of Computer Science, Imo State University, Owerri, Nigeria
[2]Department of Computer Science, Abia State Polytechnic, Aba, Nigeria
Email: Iniobongabasiama45@yahoo.com

How to cite this paper: Nwabueze, E.E. and Okon, E.E. (2019) Improved Smartphone Application for Remote Access by Network Administrators. *Journal of Information Security*, **10**, 250-262.
https://doi.org/10.4236/jis.2019.104014

Received: April 12, 2019
Accepted: October 22, 2019
Published: October 25, 2019

Abstract

This research attempts the implementation of an improved smartphone application for remote system administration. The work was motivated by the inability of network administrators to access their virtual servers from a remote location without worrying about the security implications, inaccurate and unreliable reports from a third party whenever he is out of town. The cloud server can be monitored and administered because various task such as creating users, manage users (grant access, block or delete users), restart server and shutdown server can be handled by the remote system administrator. This will involve of securing the system with a one-way hashing of encrypted password and a device ID for only whitelisted devices to be granted access. It will be observed that remote access for system administration can be implemented using a smartphone app based on a Point-to-Point Protocol and also reveal the advantages of PPP protocol, therefore making the enormous responsibilities of a remote system administrator much easier to accomplish.

Keywords

Remote Network Administrator, Smartphone App, Remote Access

1. Introduction

A computer network administrator finds it very easy to administer and monitor a network server residing in the office. Occasions arose that making the administrator unable to administer the network, such as when he is out from the office to a different location. Handling issues and knowing the status of the network become extremely difficult. The mobile smartphones which are always handy have potentials and capabilities that a network administrator can explore to monitor his network server from a remote location. These and several other issues as a matter of concern will be undertaken in this work.

Network Administrators are saddled with some responsibilities and their tasks generally will fall into four areas: Designing and planning the network, setting up the network, maintaining the network and expanding the network. Each task area corresponds to a phase in the continuing life cycle of a network. An administrator may be responsible for all the phases, or may ultimately specialize in a particular area, such as network maintenance.

The implementation of a secured system that can be administered remotely with an application that runs on Android smartphones to aid system administrator access their servers from a remote location in a situation that the administrator is out of station using their smartphones is what the study intends to accomplish.

In the opinion of Ganaa Domanaanmwi Ernest *et al.* [1], it is possible to develop an application that might enable system administrators to better monitor the status of their networks through using the proposed smartphone app and short messaging system (SMS) to perform system administration task as remotely creating users or adding users to their networks using their smartphones, creating and saving text files on a remote server running a Hypertext Pre-Processor (PHP) program, and as well-read and modify text files on a remote server using their smartphones. Ernest, however, stressed that it is not a question of whether a remote access software will be used, but which one of the available remote access software will be selected by users and how the selected product will be configured to minimize security risk. It is against this background that a comparative study on remote access technologies and software has to be conducted in order to identify the strengths and weaknesses of these remote access technologies and how these weaknesses if any can be addressed.

Karan S.B. *et al.* [2] established that initially mobile phones were developed only for voice communication but nowadays the scenario has changed; voice communication is just one aspect of a mobile phone. There are other aspects which are the major focus of interest. Two such major factors are web browser and GPS services. Both of these functionalities are already implemented but are only in the hands of manufacturers not in the hands of users because of proprietary issues, the system does not allow the user to access the mobile hardware directly. But now, after the release of android based open-source mobile phone a user can access the hardware directly. He can design customized native applications to develop Web and GPS enabled services and can program the other hardware components like camera etc.

Based on the recent capabilities of the Android phones and the driving factors for the wireless system: the need for mobility. Mobility can be viewed based on user mobility—users can communicate anytime, anywhere, with anyone and device mobility—*i.e.* devices can be connected anytime, anywhere to the network. It is possible to develop a system that will make the difficult work of a network administrator to monitor his network from a secured remote location.

Bradley Mitchell [3] in his definition stated that a server is a computer designed to process requests and deliver data to another computer over the internet or a local network.

The word "server" is understood by most to mean a web server where web pages can be accessed over the internet through a client like a web browser. However, there are several types of servers, including local ones like file servers that store data within an intranet network.

Although any computer running the necessary software can function as a server, the most typical use of the word references the enormous, high-powered machines that function as the pumps pushing and pulling data from the internet.

Ernest went further to stress the importance of remote access to a network server by the network administrator thus: One cannot down play the value that will be derived from network administrators monitoring the status of their networks through their smartphones whenever they are away from the office. It is very important to the extent that it will enable System Administrators to monitor their networks remotely through their smartphones instead of relying on third-party reports which may not even be accurate.

Sullivan Mark P. [4] reiterated an important fact that remote network administration allows network administrator to manage their networks while being physically separated from the network equipment. Having the capability to manage wired or wireless network securely, from remote locations, can substantially reduce operating expenses.

The assessment of Sullivan has further echoed the relevance of a secured remote access system for network administration, the effective and efficient actualization of a better system for network administrators. All these will in addition substantially make the enormous responsibilities of administering a network easier. This research will, therefore, provide confidence and reassurance to a remote network administrator.

This work is structured into five sections, starting from the introduction which gave a general background of the research, followed by the review of related work from body of knowledge. The third section described the research: improved smartphone application for remote system administration. Security implication vis-à-vis performance evaluation was the concern of the forth section. The next section presents the application area of remote access systems followed by Network administrators and Servers, and finally the conclusion.

2. Related Work

According to TISN [5], the ubiquitous nature of the Internet and the maturity of web-based applications have also enabled remote-access opportunities—ranging from simple communication (email and web browsing) to enabling complex industrial control systems.

Remote-access technologies are widely deployed as part of business-as-usual operational processes for the majority of organizations today. Underpinning the pervasive usage of remote-access technologies is the growth of trends including teleworking, mobile computing device adoption and web-based application delivery. All of these trends have shifted the perimeter of an organization's enterprise beyond the reach of the physical premises, allowing a worker to access business functionality and services in a manner that is consistent with working from the office—anywhere, anytime.

The Concept of Remote Access and Mobile App Techniques

Naaman & Tom [6] defined remote access as the ability to connect and gain access to internal network resources that are physically disbursed. Basically, this means that a workstation equipped with remote access software will give authorized users at the remote site access to dial in over a phone or ISDN line to read E-mail, troubleshoot problems, run applications, and transfer files to and from the corporate computers.

In their opinion, one of the successful models for remote access is the Internet-based remote access issues/solutions. The scope of this work is beyond ordinary connection between the clients and the server to access the permitted files in the server but provide the client to actually determine the functionality of the server.

For a remote access to a cloud server or traditional server, the client-server architecture has the server as a major component which serves data for clients. Request and response is the mode of communication among the client and server which is in sharp contrast with the peer-to-peer architecture that is on demand complementation in the relationship. Particularly remotely and to share resources, fundamentally any computerized process that can be used or called by another process is a server and the calling process or processes is a client.

Also observed by TISN is the growth in both the capability and number of smartphones and handheld computing devices has been phenomenal. As an illustration, Apple CEO, Steve Jobs reported in 2010 that more than 15 million iPads had been sold in nine months and that more than 100 million iPhones had been sold at that point in time. The proliferation of this category of devices indicates a strong trend that is expected to continue relating to the mobility of workers and their use of remote access as part of business as usual operations.

Ashvini & Pattalwar [7] stated that it is easy to control the network when administrator is present in the office but when the administrator is away from office then it is difficult to get the detail of network activities. It is not necessary to depend on any other third party for getting the details of the network activity. So developing a mobile application through which administrator can easily monitor and control the network activity becomes imperative.

Also, Onkar *et al.* [8] described smartphone application for system administrator as a system that client side application involves the smartphone with android application installed on it. Client side is visible to the user and users interact with client side by using some specific action and receiving the response as an outcome of that action. Server side application responsible for processing the request from client side and returns desired result to the client side. Like traditional client-server application, the android client application is installed on smartphone which is fully depends on the server application for service such as a making calls/SMS, retrieving call logs/SMS and providing operator information.

From **Figure 1** herein above, Onkar's method is based on the ability of the client to receive response from the server through SMS and acting on it which in our view is accessible to the man-in-the-middle. In contrast, this research will give the client the capability to determine how and what functionalities the server is able to perform without vulnerability to a third party based on the securities provided.

3. Design of Improved Smartphone App for System Administrators

This system is basically made of an Android Phone Application, a Cloud Server and a Database indicating the architecture of the system. This research work intends to build an android mobile application based on a secure point-to-point protocol sitting on a mobile device that will communicate with a network server.

The server will perform the processing and send response back to the android app. As an example, android app will be responsible for issuing basic commands like creating files and as well as performing basic server management task such as creating users, deleting and blocking user, setting user privileges, switching on/off the server, etc.

The responsibility of the database will be to keep track of users who log onto the system through their smartphones for audit trail purposes (**Figure 2** and **Figure 3**).

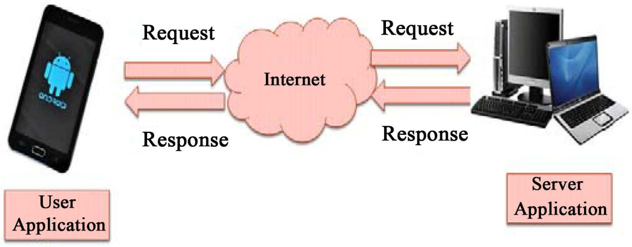


Figure 1. Client-server architecture diagram of system, Onkar *et al.* (2016).

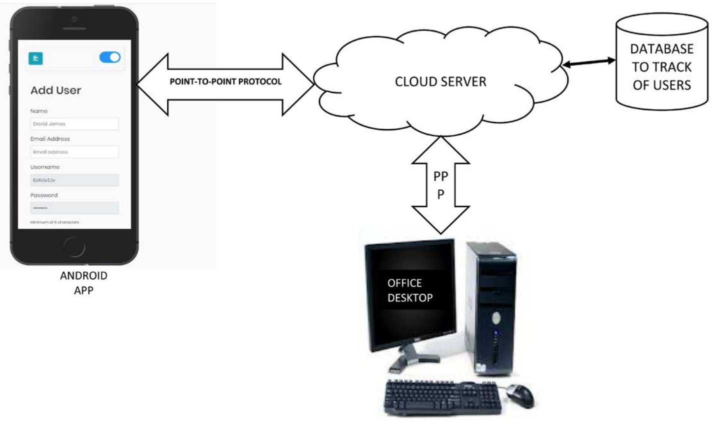
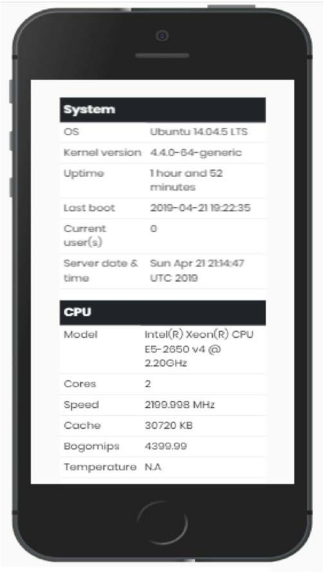


Figure 2. Architecture of remote access system.



System	
OS	Ubuntu 14.04.5 LTS
Kernel version	4.4.0-64-generic
Uptime	1 hour and 52 minutes
Last boot	2019-04-21 19:22:35
Current user(s)	0
Server date & time	Sun Apr 21 21:14:47 UTC 2019

CPU	
Model	Intel(R) Xeon(R) CPU E5-2650 v4 @ 2.20GHz
Cores	2
Speed	2199.998 MHz
Cache	30720 KB
Bogomips	4399.99
Temperature	N.A

The figure indicates the configuration of the cloud server on the smartphone.

Figure 3. Server configuration.

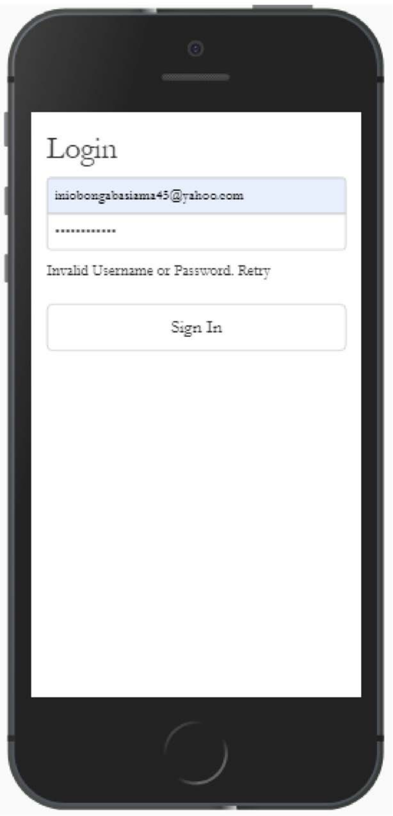
The remote administrator logs into the administrator's server using the smartphone (**Figure 4**). On a successful login the remote administrator establishes a connection between the server and the smartphone. The network administrator can create text files, create users using smartphone, view and modify text files, check the network status, monitor or administer the server, restart the server and short down the server using the smartphone from a remote location.

The remote network administrator is capable of adding users to network using his smartphone and can also remove a user from the network or block a user (**Figure 5**). The button on the top right hand side of the figure enables the administrator to shut down the server from anywhere.

The performance of the proposed improved smartphone app for system administration can be assessed as follows:

Resolution: Our remote access system is using android smartphone application with a functionality to access the entire server rather than viewing the desktop of the server, therefore extending the scope and improving the existing systems (RFB, RDP, VNC, etc.) by eliminating resolution dependency on the server and client completely.

Speed: Most of the existing access systems are based on Remote Frame Buffer (RFB) or Secured RFB protocol to transmit all information between connected devices through the updating of graphical screen display. This tends to reduce the level of accessibility in terms of speed since the server side must interpret all events received from the client and inject them into self-system. The Point-to-Point protocol deployed in the implementation of our system is capable of defining the format of the frame to be exchanged between devices, negotiate the establishment of link and the exchange of data, defining how devices authenticate themselves, and provision of services supporting a variety of network-layer protocols.



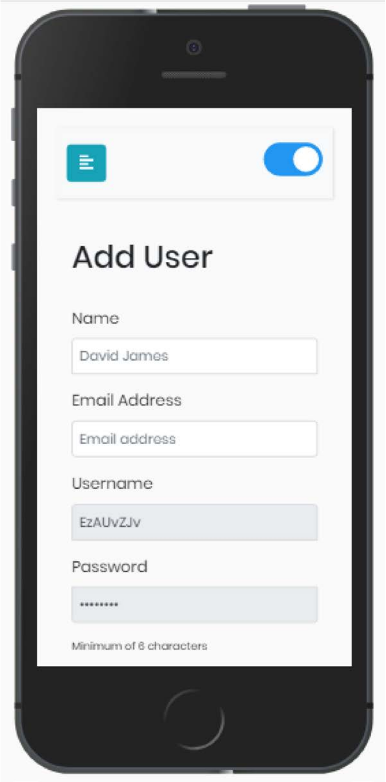
Login

iniobongabasiama45@yahoo.com

••••••••••••

Invalid Username or Password. Retry

Figure 4. User login.



Add User

Name

David James

Email Address

Email address

Username

EzAUvZJv

Password

••••••••

Minimum of 8 characters

Figure 5. Adding users by network administrator.

Security Type: A Secure RFB protocol (SRFB) with self-signed SSL certificate on top of the RFB protocol is still vulnerable to attack by man-in-the-middle due to the serial nature and idle time redundancy in RFB protocol. A whitelisted Globally Unique Identifier (GUID) provides an improved security for the client (smartphone) in our system.

4. Security Implementation

Dave Boxall [9] while commenting on Guardian stated that there is also the cloud, but when it comes to mobility, is it really your friend? While it might be a chief technology officer's (CTO) dream in terms of potential savings on storage and VPN client/server costs, the reality is that to stop data leakage some additional controls are required to prevent sensitive data migrating via the cloud to potentially insecure end user devices.

The functionality and usability of this system are to ensure that a system administrator can access his server from a remote location with adequate security on both the smartphone and the network server, and at a rate that ensures absolute availability, integrity and confidentiality of information. These are achievable based on the unique stages of authentication and verification encompassed in the system.

The first stage of security is provided by the basic components of point-to-point protocol which include:

1) Link Control Protocol (LCP) used to establish, configure, and test a PPP link;

2) Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols;

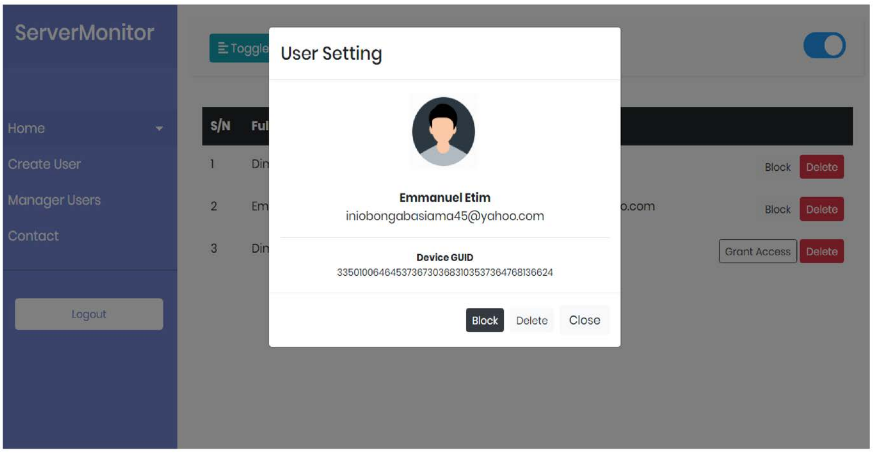
3) Authentication method used to validate the remote connection.

This is a clear distinction of our work from others because PPP is used to ensure the two point-to-point communicating parties have a reliable physical connection with each other before data is sent. Thus the PPP must establish a successful handshake between the smartphone and the server before packets are sent.

This is followed by an encrypted username and password. There is a one-way hashing of the password to avoid sniffing or eaves-dropping which prevent the Man-in-the-middle from gaining access to the network.

Finally, the system is designed such that after the verification of the user's parameters, the system then generates a unique ID, Globally Unique Identification (GUID) for the client device (smartphone) (**Figure 6**). This device unique ID is whitelisted by the server to grant user access.

Security is very important and essential in every system, whitelisting the devices involved in this research using the unique ID make our work not only secured but also compactly different from the rest. The implication is that only devices that are whitelisted can access the server. More so, once you to login using another device, your account is blocked.



User Setting

Emmanuel Etim
iniobongabasiama45@yahoo.com

Device GUID
33501006464537367303683103537364768136624

Figure 6. User management using device GUID.

Since the user can access the server using the desktop in the office and also conveniently and securely do the same from a remote location using our android application, the work is therefore seen as a hybrid system.

Performance Evaluation

In order to evaluate the performance of the Improved Smartphone Application for Remote Access by Network Administrators, the following parameters were well-thoughtout: Security, Speed in terms of accessibility and Resolution. Based on these parameters fifteen Network Administrators were interviewed and their responses analyzed.

The survey on security using GUID (Table 1) revealed that 4 of the 15 interviewees, corresponding to 26.67% indicated that the GUID is an excellent security feature for the improved system. 8 interviewee representing 53.33% stood for very good while the remaining 3 interviewee corresponding to 20.00% agreed that the security is good.

From Table 2, 2 of the interviewee representing 13.33% believed that there excellent and tremendous improvement in the accessibility in terms of speed. 6 of the 15 corresponding to 40.00% said the speed is very good and 7 indicating 46.67% response revealed good.

Performance based on the resolution of the smartphone screen (Table 3) showed that 1 person interviewed was excited with the excellent resolution, thus giving us 6.67%, 3 respondent representing 20.00% were of the opinion that the resolution is very good and 11 persons showing 73.33% believed that the resolution is good.

Although interview as a method of gathering data permitted us to get individual network administrator's view work wise and operation wise, better clarity and immediate feed, it is very time consuming, thus the size of the population.

The survey also revealed that many of the respondents do not have any knowledge about GUID and its application for security purposes. Ability to generate GUID and use it to white list the smartphones was very exciting to the respondents. From this performance evaluation respondents rating on the speed,

Table 1. Performance based on GUID.

	Frequency	Percentage	Cumulative Percentage
Excellent	4	26.67	26.67
Very Good	8	53.33	80.00
Good	3	20.00	100.00
Total	15	100.00	

Table 2. Performance based on speed of access.

	Frequency	Percentage	Cumulative Percentage
Excellent	2	13.33	13.33
Very Good	6	40.00	53.33
Good	7	46.67	100.00
Total	15	100.00	

Table 3. Performance based on screen resolution.

	Frequency	Percentage	Cumulative Percentage
Excellent	1	6.67	6.67
Very Good	3	20.00	26.67
Good	11	73.33	100.00
Total	15	100.00	

resolution and security type provided in the research makes the improves smartphone system a better option for remote system administrators.

5. Application Areas of Remote Access

A remote-access VPN allows individual users to establish secure connections with a remote computer network Jeff Tyson & Stephanie Crawford [10]. Those users can access the secure resources on that network as if they were directly plugged into the network's servers. An example of a company that needs a remote-access VPN is a large firm with hundreds of salespeople in the field. Another name for this type of VPN is virtual private dial-up network (VPDN), acknowledging that in its earliest form, a remote-access VPN required dialing into a server using an analog telephone system.

Clients and colleagues can be supported whenever they need the services of the network administrator. This will eventually reduce the administrative cost of many organizations through the elimination of duty tour allowances the administrator earned.

Applications and document can be easily accessed anytime, anywhere and with any type of device.

Remotely administer unattended computers (e.g. servers) and carryout the enormous responsibilities of a network administrator which requires you to always be in touch with the server and monitor the status of the network

Easily transfer files to and from devices whenever the need arose. This can be done without the administrator not physical present at where the server is located.

6. Network Administrators and Server

Networks, be it wide area network, metropolitan area network or local area network is an essential infrastructure in modern economy, which stimulates the development of other sectors such as commerce, industry, agriculture, education, health, banking, defense, transportation, and social interaction and that is why Teodora Bakardjieva [11] writes: "usually the server is a higher than average performance computer. The server also controls the network access of the other computers which are referred to as the "client" computers. Typically, teachers and students in a school will use the client computers for their work and only the network administrator (usually a designated staff member) will have access rights to the server".

Linfo [12] defined a server as a software program, or the computer on which that program runs, that provides a specific kind of service to client software running on the same computer or other computers on a network. The client-server model is an architecture (*i.e.*, a system design) that divides processing between clients and servers that can run on the same machine or on different machines on the same network. It is a major element of modern operating system and network design.

A computer program or a computer device endowed with the capability to provide some functionalities and assist other computer program or devices is a server. The computer program or the devices assisted with these functionalities is called the client. A network server is a computer system, which is used as the fundamental source of data, various programs and devices that are shared by users in a network.

Strictly speaking, the server is the software that handles a specific task. However, the powerful hardware that supports this software is also usually called a server because server software coordinating a network of hundreds or thousands of clients requires hardware much more robust than what you would buy for ordinary consumer use.

Rouse Margaret [13] define cloud server as a hosted, and typically virtual, computer server that is accessed by users over a network. Cloud servers are intended to provide the same functions, support the same operating systems (OSes) and applications, and offer performance characteristics similar to traditional physical servers that run in a local data center. Cloud servers are often referred to as virtual servers, virtual private servers or virtual platforms.

Alexa Huth & James Cebula [14] acknowledged that the cloud makes it possible for you to access your information from anywhere at any time. While a traditional computer setup requires you to be in the same location as your data storage device, the cloud takes away that step. The cloud removes the need for you to be in the same physical location as the hardware that stores your data. Your cloud provider can both own and house the hardware and software necessary to run your home or business applications.

This is especially helpful for businesses that cannot afford the same amount of hardware and storage space as a bigger company. Small companies can store their information in the cloud, removing the cost of purchasing and storing memory devices. Additionally, because you only need to buy the amount of storage space you will use, a business can purchase more space or reduce their subscription as their business grows or as they find they need less storage space.

7. Conclusion

This research work was able to demonstrate and also advance beyond reasonable doubt that it is very practical to deploy a system on a smartphone that can be used to support network administrators and other related professionals in their line of work to dramatically improve the services they provide to their clients or people who patronize the services they provide. The actualization of effective and secured access to a network server by the network administrator from a remote location is achievable, thus making it easy for the enormous responsibilities which require a network administrator to constantly monitor and keep the network up-to-date through this research. Further studies can be carried out on how an administrator can remotely access multiple servers with a single smartphone at the same time.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Ernest, G.D., Timothy, A.A. and Kpangkpari, G. (2016) The Use of Remote Access Tools by System Administrators Today and Their Effectiveness: Case Study of Remote Desktop, Virtual Network Computing and Secure Android App. *International Journal of Computer Applications*, **136**, 35-38.

[2] Karan, S.B., Vishnu, B.M., Akash, D.M. and Sachin, B.T. (2015) Remote Desktop Access through Android Mobiles and Android Mobiles Access through Web Browser. *International Journal of Computer Science and Information Technology Research*, **3**, 26-30. https://www.researchpublish.com

[3] Mitchell, B. (2018) Servers Are the Heart of the Internet. Lifewire. https://www.lifewire.com/bradley-mitchel-816228

[4] Sullivan, M.P. (2004) Secure Remote Network Administration and Power Management. Naval Postgraduate School, Monterey, CA.

[5] TISN (2011) Remove Access: A Tool to Support Business Continuity Planning. https://www.tisn.gov.au/Pages/default.aspx

[6] Mustafa, N. and Peltier, T. (1998) Fundamentals of Remote Access. Data Security Management. Auerbach Publications, Boca Raton, FL.

[7] Chatule, A.K. and Pattalwar, S.V. (2016) Android Based Network Monitoring and

Administration Using Wi-Fi, GPRS. *International Journal of Advances in Electronics and Computer Science*, **3**, 273-275.

[8] Mule, O., Shaikh, N., Shinde, P., Wagaskar, A. and Ramteke, S. (2016) Remote Access of Android Smart Phone. *International Journal of Computer Science and Information Technologies*, **7**, 711-714.

[9] Boxall, D. (2013) The Security Risks of Remote Working. Guardian News & Media Limited.

[10] Tyson, J. and Crawford, S. (2019) How VPN Works. Remote-Access VPN. https://computer.howstuffworks.com/vpn3.htm

[11] Bakardjieva, T. (2013) Introduction to Computer Networking. Varna Free University "Chernorizec Hrabar". Institute of Technology.

[12] Linfo (2005) The Linux Information Project. http://www.linfo.org/server.html

[13] Margaret, R. (2018) Cloud Server. Cloud Computing. Techtarget. https://www.techtarget.com/contributor/Margaret-Rouse

[14] Huth, A. and Cebula, J. (2011) The Basics of Cloud Computing Carnegie Mellon University. Produced for US-CERT.