Wireless Secured Windows System

M. Umamaheswari, S. Sivaprakash, P.U. Akhil Kumar, D. Pooja, S. Priyadharshini and S. Rubini

Abstract--- Wireless Secured System for a vendor is a web application and window software system, in terms of user can be the set the same user name and password by the program code of windows software and web application. This project analysis, the major security of the threat of locks and unlock the lock screen of the window through the WIFI connection of the applications. It should be not only function in WIFI; it can be also connected to the cloud whether by user. Cloud connectivity can be easily lock and unlock whenever we need. This security can be applicable for input function of the system; it can be also able and disable the working function of the mouse and keyboard. User to enter the user name and password in the web page, it send as the WIFI code to Servlets, and intermediate request send to the windows application by the Servlets, and back ground function a as windows software to implement the security functions. Aimed using the WIFI and cloud computing, network user to establish the secure network application platform.

Index Terms--- Wi-Fi, Web-Server, System Application, Cloud Computing, Computer Security, Mobile Communication.

M. Umamaheswari, Assistant Professor, Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, Namakkal. E-mail:umadeena@gmail.com

S. Sivaprakash, Assistant Professor, Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, Namakkal. E-mail:shivaiter@yahoo.co.in

P.U. Akhil Kumar, UG Scholar, Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, Namakkal. E-mail:akhil.kumarcse@ksrce.ac.in

D. Pooja, UG Scholar, Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, Namakkal. E-mail:pooja.dcse@ksrce.ac.in

S. Priyadharshini, UG Scholar, Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, Namakkal. E-mail:priyathangam96@gmail.com

S. Rubini, UG Scholar, Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, Namakkal. E-mail:rubirubini2014@gmail.com

I. INTRODUCTION

The world is running faster than the clock, more than the hard work and smart work is getting successes in today's world. Among them a computer's are smarter. Throughout the world humans are using the system application (any device), to do their works and not only work is done with the devices but also studies, chatting (social media), reading news, entertainment etc…, activities are done by using an system. So, probably the information (personal info, authorized info) is stored in the personal system.

The owner of the device will be keeping their property (device) with the secured password. A device with a password will open when the correct password is entered. Security of the personal device is what being discussed. In this paper wireless secured window system is been thought to secure the system. These can be easily used by malicious users (e.g., criminals, terrorists and business spies). Wireless security has attracted a lot of research interest in the literature. As shown in Fig. 1, wireless application includes mobile ad hoc networks by exploiting wi-fi and cloud.

II. EXISTING SYSTEM

The existing system is used to set username and password manually to lock and unlock the windows application.

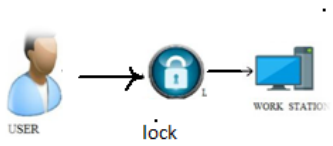

Figure 1: Existing System

This security can be inbuilt by the system till windows 10. In the other system (system application), picture

security is used it can be set the password and accessed by the click by the mouse pointer at required place of the picture to unlock the lock screen.

Last year Microsoft introduced the finger print sensor to unlock the system as shown in Figure 1. (Existing system). User can keep the finger print in the finger scanning board to set the finger print in the scanner as shown in Fig. System can be scanning the finger to unlock the system. Third party can access the application easily, because it is less secured by using pin or password. At least one user should be available in the system.

III. RELATED WORKS

In the literature, there have been a handful of methods for eavesdropping infrastructure-based communications (e.g., cellular networks). Nevertheless, they cannot be efficiently applied to infrastructure-free mobile communication networks. On the other hand, passive eavesdropping, which has been conventionally investigated has malicious attacks in the wireless security literature [1].

There are also some studies on active jamming attacks to intrude on and disrupt targeted wireless receivers. For instance, constant, intermittent, reactive, adaptive jamming schemes, in which Gaussian noise is artificially generated as the jamming signals to interfere with the targeted receivers [6].

The term mobile cloud computing (mcc) was introduced not long after the concept of the ‘cloud computing’. It has been attracting the attentions of entrepreneurs as a profitable business development, of mobile users as a new technology to achieve grate services [14].

In this article device to device (D2D) communication under laying a 3GPP LTE-advanced cellular networks is studied as an enalber local service with limited interface impact on the primary cellular networks[3].

IV. PROPOSED SYSTEM

Wireless Secured System working under by the web-application and windows software of the system. The system can be secured the pin or password of the WI-FI connection between the web page and the windows application [2]. Web application can control through web server (mobile-.server). User can be send the request through WI-FI by web page of the mobile, request can accept by back end of the function as shown in Figure 2. (Proposed system). And the request matches to the windows application to unlock the system. And same way to lock the system by request of the user sends to the backend.

It’s also can be work in the cloud function to lock and unlock the system. This security can be able and disable the working function of the mouse and keyboard. User can able to lock and unlock with mobile. We can be able and disable the working function of the mouse and keyboard.

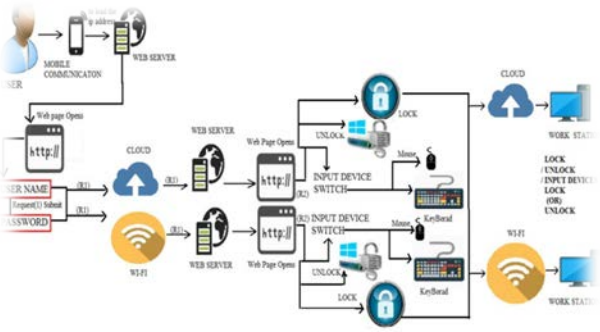

Figure 2: Proposed System

This system can be also work in the cloud to secure the system. In required distance we can secure the system through WI-FI. Third party cannot access WI-FI password. Third party cannot unlock system pin or password.

Security of System

The system is secured when there is no interruption of the third parties. As a response, there is a growing need for authorized parties to secure public, commercial, and military. There, is lots of upcoming system application which is secured by its inbuilt security system. Such as, face recognize, finger print. There is a solution for any type of system it is the wireless communication and cloud

computing, as shown in Figure 3. (Mobile ad hoc network and Wi-Fi and cloud).

Figure 3: Mobile Ad Hoc Network and Wi-Fi via Cloud

It has a security, as for an example if the third party accesses your computer and they can misuse with your data or personal information[8], but he cannot misuse because the user has the controlled their device with the web server (mobile or any other web application) by turning on the lock device user secure that screen were third party cannot threat with and other input device (hack).

Wireless Infrastructure

The wireless requires a large number of densely deployed surveillance and invention "dogs" (SIDs) to eavesdrop and them, as these uses are likely to be located anywhere and move from one location to another [4], as show in Fig 4.(mobile ad hoc network and wireless communication) . It is worth nothing that some specific infrastructure-free from suspicious and malicious wireless communication and cloud computing [6]. There have been a handful of methods for eavesdropping infrastructure –based communications (e.g., cellular networks).

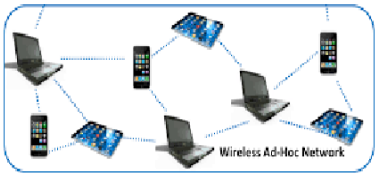

Figure 4: Mobile Ad Hoc Network and Wireless Communication

For example, the NSA has deployed dedicated wiretapping devices in networks [11] operators can install monitoring software such as FlexiSPy http://www.flexispy. com) in targeted smart phones. Nevertheless, they cannot be efficiently applied to infrastructure-free mobile communication networks [1], it is applicable to intercept infrastructure-free wireless communications.

Cloud Infrastructure

Together with an explore growth of the mobile applications and emerging of cloud computing concept. Mobile devices (e.g., Smartphone and tablet PC) are increasingly becoming a part of human life as the most effective and convenient communication tools not bounded by time and place. The rapid progress of mobile computing (mc) becomes a powerful trend in the development of IT technology as well as commerce and industry fields [13].

Cloud computing (cc) has been widely recognized as the next generation infrastructure (e.g., Server, networks, Storages), platforms (e.g., Middleware services and operating Systems), and software (e.g., application program) provided by cloud provider (e.g., Google, Amazon, Salesforce) at low cost [12].

Cloud Computing with Mobile Connecting

Cloud enables users to elastically utilize resource in an on-demand fashion. As, a result, mobile applications can be rapidly provisioned and released with the minimal management efforts or services provider's interactions [11]. In this, paper the cloud is used as the server, were the user on another hand uses a cloud server for operating the devices.

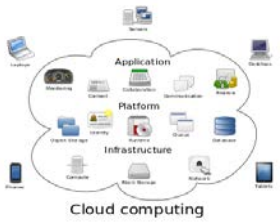

Figure 5: Connecting with Cloud Infrastructure

The user will connect with to the cloud and get the IP address for maintaining their devices, he/she can login (with the address is already on their application it will generate a IP address (link) as shown in the Fig 5. (connecting with cloud infrastructure) and also the username and password is

set on the backend) to cloud and enter the username and password if both the password matches it will move to the next page, were user can lock the screen and input devices.

The term mobile cloud computing (mcc) was introduced not long after the concept of the 'cloud computing'. It has been attracting the attentions of entrepreneurs as a profitable business development, of mobile users as a new technology to achieve grate services [14]. It presents several issues that arise in MCC and approaches to address issues. Mobile devices are connected to the mobile network via base stations (e.g., base transceiver station, access point, or satellite)

Cloud Security

Cloud computing system and services have become major targets for cyber attackers. To provide strong protection of cloud platforms, infrastructure, host application, data stored in cloud[11]. The practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.

Surveillance Privacy

Beyond technology, the user privacy issue related to our surveillance solution may be a critical public concern. Nevertheless, the proper use of surveillance can indeed help protect legitimate users privacy from malicious users [9].

V. CONCLUSION

Wireless secured system is the new thought of securing the personal device. That will ensure the user and satisfies that his/her data's and information is protected from the malicious users. User is able to control their device either he/she is near to the device are far from the it they can control their device through the web server (mobile phone) they can lock their device when it is not used(by clicking on the lock button of the inputs and the screen). This aims to defend against illegal eavesdropping and malicious.

REFERENCES

[1] Y. Zou, J. Zhu, Wang, X and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends", Proc. IEEE, Vol.104, No. 9, Pp. 1727–65, 2016.

[2] G. Nardini, G. Stea, A. Virdis, D. Sabella and M. Caretti, "Broadcasting in LTE-Advanced networks using multihop D2D communications", IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Pp. 1-6, 2016.

[3] S. Bi, R. Zhang, Z. Ding and S. Cui, "Wireless communications in the era of big data", IEEE communications magazine, Vol. 53, No. 10, Pp. 190-199, 2015.

[4] M. Chen, S. Mao and Y. Liu, "Big Data: A Survey", Mobile Net. Appl., Vol. 19, No. 2, Pp. 171–209, 2014.

[5] J. Xu, L. Duan and R. Zhang, "Proactive Eavesdropping via Jamming for Rate Maximization over Rayleigh Fading Channels", IEEE Wireless Commun. Letters, Vol. 5, No. 1, Pp. 80–83, 2016.

[6] Y. Zeng and R. Zhang, "Wireless Information Surveillance via Proactive Eavesdropping with Spoofing Relay", IEEE J. Sel. Topics Signal Process., Vol. 10, No. 8, Pp.1449–61, 2016.

[7] J. Xu, L. Duan and R. Zhang, "Transmit Optimization for Symbol-Level Spoofing with BPSK Signaling", IEEE Globecom Workshops (GC Wkshps), Pp. 1-6, 2016.

[8] M.H. Manshaei, "Game Theory Meets Network Security and Privacy", ACM Comp. Surveys, Vol. 45, No. 3, Pp. 1–25, 2013.

[9] G.T. Marx, "Surveillance Studies", Int'l. Encyclopedia Social & Behavioral Sciences, 2nd ed., Vol. 23, Pp. 733–41, 2015.

[10] G.H. Forman and J. Zahorjan, "The challenges of mobile computing", IEEE computer society magazine, Vol. 27, No. 4, Pp. 38-47, 1994.

[11] M. Alie, "Green cloud on the horizon", Proceeding of the 1st international conference on cloud computing (cloud coom), manila, Pp. 451-459, 2009.

[12] R.N. Calheiros, C. Vecchiola, D. Karunamoorthy and R. Buyya, "The Aneka platform and QoS-driven resource provisioning for elastic applications on hybrid Clouds", Future Generation Computer Systems, Vol. 28, No. 6, Pp. 861-870, 2012.

[13] R. Buyy, C.S. Yeo, S. Venugopal, J. Broberg and I. Brandi, "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility", Journal on future generation computer system, Vol. 25, No. 6, Pp. 599-616, 2009.

[14] A. Rudenko, P. Reiher, G.J. Popek and G.H. Kuenning, “Saving portable computer battery power through remote process execution”, ACM SIGMOBILE Mobile Computing and Communications Review, Vol. 2, No. 1, Pp. 19-26, 1998.