International Journal of Innovative Research in Engineering Science and Technology

APRIL 2018 ISSN 2320 –981X

USER LOGIN SYSTEM SECURITY THROUGH MOBILE

[1]Mr.Karuppusamy.E, [2]Ms. Mohanapriya.G.K, [3]Ms.Monika.S

1.Department of Computer Science and Engineering,
SNS College of Technology
Coimbatore-641035
karuppusamyeskk@gmail.com

2.Department of Computer Science and Engineering,
SNS College of Technology
Coimbatore- 641035
gkmohanapriyavkl@gmail.com

3.Department of Computer Science and Engineering,
SNS College of Technology
Coimbatore- 641035
moni738497@gmail.com

CORRESPONDING AUTHOR:
Mr.C.B.Sivaparthipan
AP/Dept. of Computer Science and Engineering
SNS College ofTechnology
Coimbatore-641035
sivaparthipanece@gmail.com

Abstract- Nowaday's personal computers and mobile phone are commonly available with everyone.Security for the personal computer is must to protect the valid informations.In this paper,we will discuss the System Security through Mobile in which program is stable when running under windows.It will be helpful to control our personal computer through USB authentication. In the mobile security access command have to be typed in the pc and connected number must be connected to a system through a data cable. In Personal Computer user connected with smartphones and their corresponding data cable. If the pc need to be controlled then the user must know the Mobile Number of which is connected to pc. The application done all mobile processes by using AT (Attention) commands.Data regarding the user are collected and maintained for secured process.The main objective is to automate to access system operations through USB authentication and easy retrieval of the stored data. Reports have been generated for the purpose of maintaining user's mobile details and operations details.

1.INTRODUCTION

In mobile computing, Mobile security has become increasingly important.The security of personal and business information are now stored on smartphones.More users and business people have use smartphones to communicate, but also to plan and organize their work and for their private life.Moreover these technologies are causing extreme changes in the organization of information systems.Smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company.In the existing system there is only manual process for controlling the Pc, also it has more workload for the authorized person, but in the case of Proposed System, the user can get in the application and checks the information for places or about a particular places are in the paper works to get to control the Pc.

All smartphones, as computers, are preferred targets of attacks.In communication mode—like Short Message Service (SMS), Multimedia Messaging Service (MMS), wifi, Bluetooth and GSM, the de facto global standard for mobile communications, there are attacks which exploit weaknesses inherent in smartphones. In the browser or operating system there are also exploits that target software vulnerabilities.Some malicious software relies on the weak knowledge of an average user.In 2018,McAfee found11.6% users had heard of people were affected by mobile malware, but only 2.1% had personal experience on such problem. From security in different layers of software to the dissemination of information to end users security countermeasures are being developed

and applied to smartphones,. Through the development of operating systems, software layers, and downloadable apps There are good practices to be observed at all levels, from design to uses.

2.EXISTING SYSTEM

In the existing system there is only manual process for control the Pc is availed, and also it has more workload for the authorized person, but in the case of Proposed System, the user can get in the application and checks the information for places or about a particular places are in the paper works to get to control the Pc.

2.1 Drawbacks of Existing System

The limitations of available systems are only manual process for control the PC is available, also it has more workload for the authorized person. In this section, we present some of the limitations that are present in the existing system.

1) More manual steps.
2) Time consuming.
3) Consumes large volume of system work.
4) Needs manual routes information.
5) No direct data given for the users.
6) To avoid all these limitations to find the places and make the working more accurately the system needs to be computerized in a better way.

The proposed method helps to eliminate all the drawbacks mentioned above.

3. PROPOSED SYSTEM

To develop a system of improved facilities is the main aim of proposed system The limitations of the existing system can be overcome by the proposed system. The difficulties can be able to eliminate or reduce to some extent and simplifies by using the User's personal mobile. The proposed system will help the user to reduce the workload and improved the security by authenticating through this mobile. The main advantage is that the system is very simple in design and to implement.The system will work in almost all configurations and requires very low system resources. There is no need to use the external software and the file is in protected state.

3.1 Advantages of proposed system

It has got some features which are listed below:

1) Maximize the security Level.
2) Minimum time needed for the various processing.
3) Greater efficiency.
4) Better service.
5) User friendliness and interactive without internet.
6) Minimum time required.

4.PROJECT DESCRIPTION

4.1.VISUAL STUDIO .NET

The Visual Studio 2010 IDE was upgraded which agreeing to Microsoft, clears the UI association and "decreases mess and multifaceted nature". The new IDE better backings different record windows and drifting instrument windows,while offering better multi screen bolster. The IDE shell has been changed utilizing the Windows Presentation Foundation , whereas the internals have been overhauled using Managed Extensibility Framework that offers more extensibility points than past renditions of the IDE that empowered add-ins to adjusttheconductoftheIDE.Itsupports IBMDB2 and Oracle databases,notwithstanding Microsoft SQL Server. It has incorporated help for developing Microsoft Silver light applications, including an intuitive architect. Visual Studio 2010 offers few instruments to make parallel programming simpler:notwithstanding the Parallel Extensions for the .NET Framework and the parallel designs Library for native code.

Visual Studio 2010 incorporates devices for troubleshooting parallel applications. The new devices permit the representation of parallel Tasks and their runtime stacks.

Devices for profiling parallelapplications can be used for representation of string hold up times and string movements crosswise over processor centres. Intel and Microsoft have mutually promised help for a another Concurrency Runtime in Visual Studio 2010 and Intel has propelled parallelism bolster in parallel studio as an extra for Visual Studio. Visual Studio 2010 Service Pack 1 was discharged in March, 2011. The .Net Framework is a dialect impartial stage for composing programs that can without much of a stretch and safely interoperate. There is no dialect boundary with .Net there are numerous dialects available to the engineer including Managed C++, C#, Visual Basic and Java Script.

".Net" is additionally the aggregate name given to different programming segments based upon the .Net stage. These will be two items (Visual Studio.NET and Windows.NET Server, for example) and administrations (like Passport, .NET My Services, And so on).The .NET Framework has two principle parts are the Common Language Runtime and the .NET Framework class library.

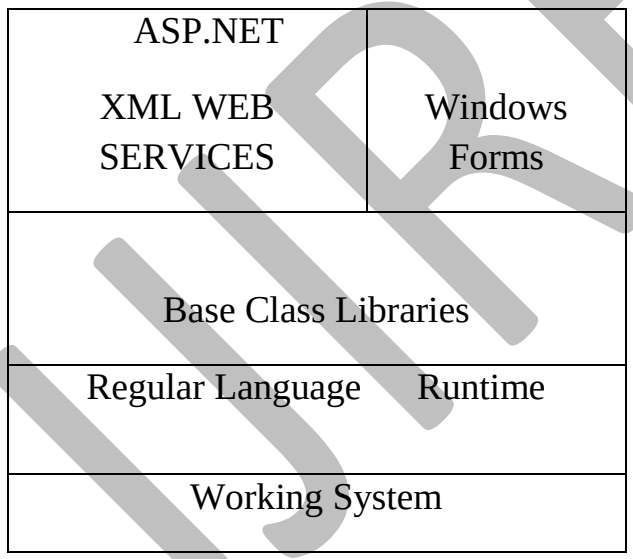

Fig.1: .NET Framework

The multi-dialect capacity of the .NET Framework and Visual Studio .NET empowers engineers to utilize their current programming aptitudes to manufacture a wide range of utilizations and XML Web administrations. The .NET structure underpins new forms of Microsoft's old top choices Visual Basic and C++ (as VB.NET and Managed

C++), yet there are additionally various new options to the family. Visual Basic .NET is additionally CLS consistent, which implies that any CLS-aggreable dialect can utilize the classes, articles, and parts make in Visual Basic .NET. Overseen Extensions for C++ and ascribed writing computer programs are only a portion of the improvement made to the C++ dialect.Overseen Extensions disentangle the assignment of moving existing C++ applications to the new .NET Framework.C# is Microsoft's new dialect. It's a C-style dialect that is basically "C++ for Rapid Application Development".Not at all like different dialects, its determination is only the syntax of the dialect.It has no standard library of its own, and instead has been outlined with the expectation of utilizing the .NET libraries as its own.

Microsoft Visual J# .NET gives the most effortless change to Java-dialect designers into the universe of XML Web Services and significantly enhances interoperability.Java-dialectprograms with existing programming written in an assortment of other programming languages.Other dialects for which .NET compilers are accessible include:

1) FORTRAN
2) COBOL
3) Eiffel

3.2MY SQL SERVER

SQL Server 2008 was discharged on August 6, 2008 and expects to make information management self-tuning, self arranging, and self keeping up with the advancement of SQL Server Always On technologies, to give close to zero downtime. SQL Server 2008 likewise incorporates bolster for structured and semi-organized information, including advanced media groups for pictures, sound, video and other sight and sound information. In current renditions, such interactive media information can be put away as BLOBs (binary huge items), however they are non specific piece streams. SQL Server 2008 can be an information stockpiling backend for different assortments of information: XML, email, time/timetable, record, report, spatial, etc as well as perform search, question,

investigation, sharing, and synchronization across all information types.Working with SQL server utilizing visual studio.NET, there is no compelling reason to open the Enterprise Manger from SQL Server. Visual Studio.NET has the SQL Servers tab inside the Server Explorer that gives a rundown of the considerable number of servers that are associated with those having SQL Server on them. Opening up a specific Server tab gives three choices from the accompanying: DatabaseDiagrams,Tables,Views,Query, Form, Report.

5.LITERATURE SURVEY

5.1 Mobile Application security platform survey

Nowadays Smartphone and other mobile devices have become incredibly important in every aspect of our life. Because they have practically offered same capabilities as desktop workstations as well as come to be powerful in terms of CPU (Central processing Unit), Storage and installing numerous applications. Therefore, Security is considered as an important factor in wireless communication technologies, particularly in a wireless ad-hoc network and mobile operating systems. Moreover, based on increasing the range of mobile application within variety of platforms, security is regarded as on the most valuable and considerable debate in terms of issues, trustees, reliabilities and accuracy. It aims to introduce a consolidated report of thriving security on mobile application platforms and providing knowledge of vital threats to the users and enterprises. Furthermore, various techniques as well as methods for security measurements, analysis and prioritization within the peak of mobile platforms will be presented. Additionally, increases understanding and awareness of security on mobile application platforms to avoid detection, forensics and countermeasures used by the operating systems. Finally, it also discusses security extensions for popular mobile platforms and analysis for a survey within a recent research in the area of mobile platform security.

5.2Mobile security catching up revealing the nuts and bolts of the security of mobile devices

Currently Smartphone and mobile devices have become incredibly important among people around the world. Because they have offered same capabilities as well as facilities that desktop works stations have provided. However, security aspect still is a big Challenge. Nowadays, the numbers of attackers and malicious programs have increased rapidly. According to threats predictions report 2015 will the turning point for threats to

mobile devices in which the total number of mobile malware samples exceeded 5 million in Q3 2014. Therefore, security requirements and issues within various mobile platforms become a targeted area of many studies and researches. Thus, one of the most essential decisions within the use of Smartphone is the selection of suitable mobile platforms. Generally, confidentiality, integrity and availability are three fundamental categories of the security goals and objectives of information in an organization. More to say, security can be measured through: confidentiality, integrity, authentication and authorization. Moreover, risk analysis is also considered as one of the main crucial factors within security of mobile platforms. In addition to these, when security issues and gaps are subsisted, it is crucial to identify the challenges against existed security issues. Due to incredible increasing of memory, data transmission and processing the security incident turned into be more powerful on mobile platforms and phone devices.

5.3 A Comparision of security requirements engineering methods

It focuses on security in mobile application platforms and techniques for analysis and prioritization of security requirement in terms of theory rather than technical descriptions. Furthermore, the analysis and evaluation of the existing techniques and studies will be presented. This study introduces both generic model security architectures and threat model of mobile platforms within two major known platforms of iOS and Android. The last but not the least, the security issues and privacy in mobile platforms will be also discussed. It is worth mention that security in mobile platforms has been analyzed in different perspectives in which it identify how both iOS and Android platforms has implemented security models against threats. The Background of mobile platforms, section IV introduces mobile application security platforms, namely the (i) the Rational behind securing mobile application platforms, and (ii) security threats measurements. Finding and evaluation are provided in section V and VI respectively. Mobile application development in various platforms is based on functional and non-functional requirements. Currently various types of platforms are exist to deploy mobile applications with different private policies. Therefore, this research focuses on the most priceless and popular mobile application platforms in the worldwide. Furthermore, it discusses that how the security within each platform is different from each others for instance, Motion BlackBerry OS, Apple iOS, Google Android, Microsoft Windows Phone. There are some of the imperative security issues to be evaluated and studied such as battery capacity limitation and encryption algorithms power consumption, were having major impacts on mobile devices. In addition to these, controlling third-party application

is difficult task within each mobile apps store, which they have huge impacts on increasing the security issues within mobile platforms. Dimensional Research institution in stated that Android trusted less; Windows Mobile and BlackBerry trusted more for security. Meanwhile, based on the same survey or report accordingly, most of participants believed that the security risks were the major cause of the mobile security platforms.

6.METHODOLOGY

6.1 REGISTRATION

The user must entering into the application by making the registration. When the registration is finished using creating the user profile. In registration some field are to be mentioned definitely. The password is to be mentioned and need to reentry the password again for the conformation. This process is the initial process and can further used for login purposes. While registration some restriction are specified while mentioning the details in the registration process.

6.2 LOGIN

Login authentication is only done after the registration. The application provides the authorization only after the registration. This process requires a filed like user name and password. In computing, a login session is the period of activity between a user logging in and logging out of a (multi-user) system. On Unix and Unix-like operating systems, a login session takes one of two main forms:When a textual user interface is used, a login session is represented as a kernel session a collection of process groups with the logout action managed by a session leader. Where an X display manager is employed, a login session is considered to be the lifetime of a designated user process that the display manager invokes is a long-running bi-monthly technical journal published by the usenix Association, focusing on the operating system and system administration in general. Login is published six times per year and is the membership benefit. Single issues as well as subscriptions are available for purchase to non-members. Online issues of login: more than one year old are freely available for everyone to download, as are a number of articles in each issue. Currently, issues from 1997 through the present are available online. The leading semicolon is a reference to the appearance of the login prompt of early versions, where an escape code specific to the Teletype model computer terminal would appear as a semicolon on other models of terminal. out of a system, especially not on a public computer, instead one should explicitly log out and wait for the confirmation

that this request has taken place. Logging out of a computer when leaving it is a common security practice, preventing unauthorized users from tampering with it. There are also people who choose to have a password-protected screensaver set to activate after some period of inactivity, requiring the user to re-enter his or her login credentials to unlock the screensaver and gain access to the system.

6.3ADMIN CONTROL Administrative controls are training, procedure, policy, or shift designs that lessen the threat of a hazard to an individual. Administrative controls typically change the behavior of people (e.g., factory workers) rather than removing the hazard or providing personal protective equipment (PPE).Administrative controls are fourth in larger hierarchy of hazard controls, which ranks the effectiveness and efficiency of hazard controls. Administrative controls are more effective than PPE because they involve some manner of prior planning and avoidance, whereas PPE only serves only as a final barrier between the hazard and worker. Administrative controls are second lowest because they require workers or employers to actively think or comply with regulations and do not offer permanent solutions to problems.

6.4 USER CONTROL A User Control is a separate, reusable part of a page.The piece of a page in a User Control, and then reuse it from a different location. The name, User Control, might seem a bit fancy, but actually, it's just like a regular page, with an optional Code Behind file. A notable difference is that User Controls can be included on multiple pages, while a page can't. User Controls are used much like regular server controls, and they can be added to a page declaratively, just like server controls can. A big advantage of the User Control is that it can be cached, using the Output Cache functionality described , so instead of caching an entire page, the cache only the User Control, so that the rest of the page is still re-loaded on each request.

7.FUTURE WORK

An aggressor needs three things: technique—the ability and information to play out an effective assault; opportunity—time and access by which to assault; and thought process—motivation to need to assault. Tsk-tsk, none of these three is hard to come by, which implies assaults are inevitable.applying better security instruments ought to be set up amid application signing.Further training for client about how to utilize portable

wellbeing observed to be critical to debase the quantity of information lose,attacks and in addition dangers.

CONCLUSION

Versatile security endeavors to guarantee the classification, uprightness, and accessibility of processing frameworks and their segments. Three key parts of a figuring framework are liable to assaults: equipment, programming, and information. These three, and the correspondences among them, are defenseless to PC security vulnerabilities Security circumstances emerge in numerous regular exercises, albeit now and then it can be hard to recognize a security assault and a normal human or innovative break down.A risk is an episode that could cause hurt. A helplessness is a shortcoming through which damage could happen. These two issues consolidate: Either without alternate causes no mischief, yet a danger practicing a weakness implies harm. To control such a circumstance, we can either square or reduce the risk, or close the powerlessness (or both). Now and again we neglect to perceive a risk, or different circumstances we might be not able or unwilling to close a powerlessness.

REFERENCES

[1]. Asokan, N., Davi, L., Dmitrienko, A., Heuser, S.,Kostiainen, K., Reshetova, E., Sadeghi, A. (2014) _Mobile Platform Security', Morgan & cLaypool publishers.

[2]. Becher, M., Freiling, F., Hoffmann, J., Holz, T., Uellenbeck, S. and Wolf, C. (2011) _Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices'. 2011 IEEE Symposium on Security and Privacy.P 96-111.

[3]. Benjamin, F., Seda, G., Maritta, H., and Holger, S. (2010)_A comparision of security requirements engineering methods, International Journal of Computer Applications (0975 – 8887) Volume 133 – No.2, January 2016 45.

[4].Bhattacharya,P.,Yang,L.,Guo,M.,Qian,K.,andYang,M.(2014), Learning Mobile Security with Labware', Security & Privacy.

[5]. Braun, P., and Rossak, W. (2005). _Mobile agents. Basic concepts, mobility models and the tracy toolkit'. dpunkt. verlag.

[6]. Bürkle, A., Hertel, A., Müller, W. and Wieser, M. (2008) ―Evaluating the security of mobile agent platforms' Springer Science+Business Media, LLC 2008.

[7]. Certic, S. (Not Given), _The Future of Mobile Security‘, CS Network Solutions Limited, [online]. Available at: http://www.cs-networks.net [Accessed 4th September 2014].

[8]. Chen, M. (Not given), A methodology for building mobile computing applications, USA.

[9]. Clarke,N. & Furnell, S. (2007). _Advanced user authentication for mobile devices‘. Computers & Security, vol.26, (2), pp. 109-119 [online]. Available:http://www.sciencedirect.com.libaccess.hud.ac.uk/science/article/pii/S0167404806001428 [Accessed 7th May 2014].

[10].Delac, G. Silic, M. and Krolo, J. (2011), Emerging Security Threats for Mobile Platforms‘ MIPRO 2011, May 23-27, 2011, Opatija, Croatia.

LIST OF FIGURES