

MIND METRICS

Vanitha Lam*

VenkatraoTadisetti**

Article Info

Article history:

Receivedxxxx, 2015

Revised xxx, 2015

Accepted xxx, 201x

Keywords:

Authentication,
identification, verification,
data, login id, Password,
security,embedded
systems.

ABSTRACT

The process of authenticating a computing system contains two parts namely: i) Identifying and ii) verifying. Now a days login ID's are being used for identification and password verification. Many theories have been proposed to improve this process, but they require specialized device which are not always available. The proposed method uses the current password based system by strengthening the identification process. It utilizes personnel secret data instead of a login id to identify a user uniquely, hence MIND METRICS. This total paper is to provide security using embedded systems.

* Department of Electronics and Communications Engineering, Lingaya's Institute of Management and Technology

** Asst.Prof, Department of Electronics and Communications Engineering, Lingaya's Institute of Management and Technology.

I. Introduction

It asks the user to choose a correct login ID among multiple choices of partially obscured IDs. Since it does not accept a login ID during the authentication process, a stolen or cracked password cannot be used for gaining an access to the computing system unless the attacker provides a correct identification material, i.e., mind metrics token. This additional step raises the security of an authentication system considerably over single or double password systems. Since the stolen passwords cannot be used immediately by the attackers, account holders can have extra time to change their passwords before the attackers gain an access. This scheme does not require any specialized hardware and can be implemented easily. It may be used where biometrics schemes cannot be used cost-effectively, e.g., on public e-commerce web sites. Mind metrics scheme separates the server and the verification server, thus it is scalable to a large system. We implemented a proof-of-concept system and evaluated it with test users.

II. System Block Diagram and Description

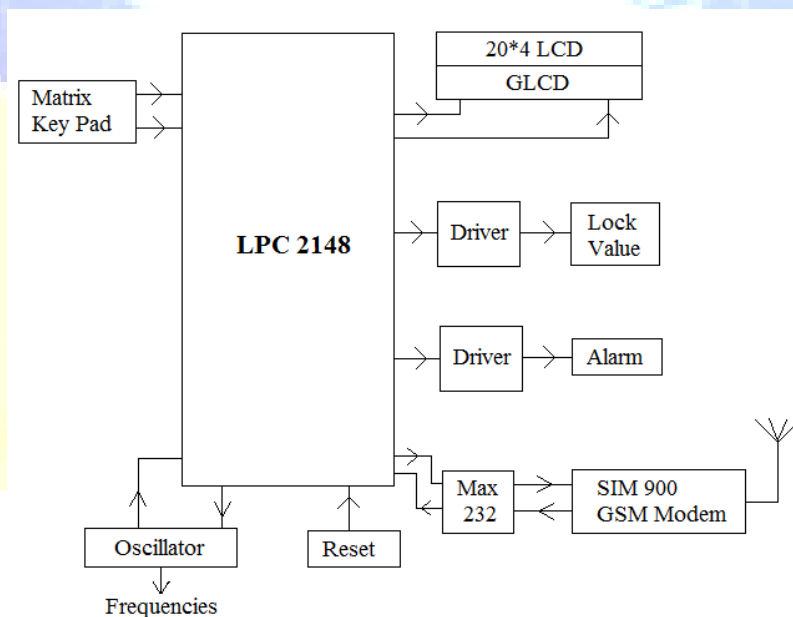


Figure 1: Block diagram

LPC2148 Micro Controller:

In this project micro controller is used to control all the peripherals. LPC2148 is used as MCU in this design. Because of the advanced 32 bit architecture, it can detect changes as low as 3 millivolts and more faster when compared to PIC's and other 80series micro controllers. Inbuilt ADC was an added benefit of LPC2148. Hence we used this as our micro controller unit .A Microchip microcontroller LPC2148 is used to collect and process data and then stores it in a serial buffers. The LPC2148 is an 32k instructions program buffers, 512 kb bytes of RAM, three timers, and a 32 -bit A/D converter microcontroller. It has RISC architecture and can use oscillators, thus it is ideal to be used as an embedded system.



Figure 2:LPC 2148

Matrix Keypad:

In matrix keypad token numbers are given as input. This is a 4*4 keypad. Typically one port pin is required to read a digital input into the controller. When there is a lot of digital input that has to be read, it is not feasible to allocate one pin for each of them. This is when a matrix keypad arrangement is used to reduce the pin count. Therefore, the number of pins that are required to interface a given number of inputs decreases with increase in the order of the matrix.



Figure 3: Matrix Keypad

MAX232:

It acts as a mediator between micro controller and GSM modem. It converts RS232 format to TTL format .The MAX232 device is a dual driver/receiver that includes a capacitive voltage generator to supply EIA-232 voltage levels from a single 5-V supply. Each receiver converts EIA-232 inputs to 5-V TTL/CMOS levels. These receivers have a typical threshold of 1.3 V and a typical hysteresis of 0.5 V, and can accept ± 30 -V inputs

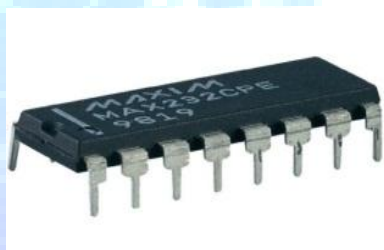


Figure 4: Max 232

GSM:

GSM modem gives capability to send SMS without any mobile operating system. SIM can be read with MCU and can be used to send SMS by micro controller. Hence a GSM modem was employed, its main function here was when the parameters are over threshold limits it sends a text message to predefined contacts about the situation of the patient, thus alerting them to proceed for further actions.



Figure 5: GSM

III. Working

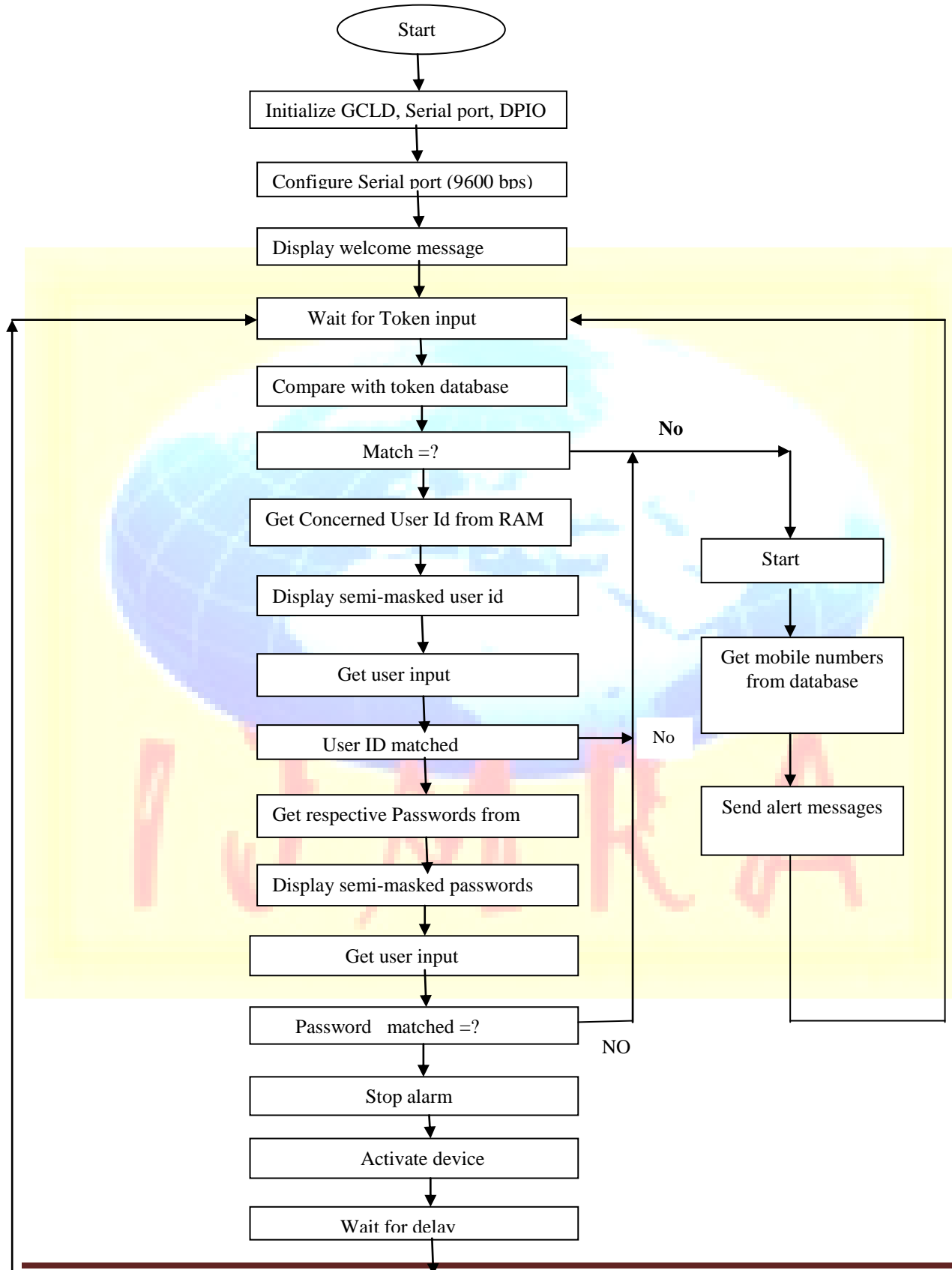
The designed system comprises of matrix keypad, LPC2148 micro controller, MAX 232 and a GSM modem. At first, we should give the token numbers as an input to matrix keypad hereby, the command is sent to LCD using micro controller (LPC2148). It displays four user names and again the command is sent back to the keypad to choose one of the username. Similarly, the password is also chosen using the above process. Sometimes if any interrupt is occurred in the process GSM the alarm will be activated. In this project MAX232 acts as a mediator between micro controller and GSM modem. It converts RS232 format to TTL format. The MAX232 device is a dual driver/receiver that includes a capacitive voltage generator to supply EIA-232 voltage level



Figure 6: Working

IV. Flow Chart

Firstly initialising the GLCD, GPIO and serial port and configuring the serial port is done. After that a welcome message is displayed on LCD and then the system waits for token input, compares with token database, if the token input matches then it will get concerned user ID from RAM, displays semi masked user ID, gets user input and if the user ID matches then it displays respective passwords from RAM, displays semi masked RAM and if the password is also matches then the system activates. And if either of the token or user ID or password does not match then the alarm will be ON and sends an alert message.



IV. Conclusion

User authentication is done in two steps, identification and verification. The traditional password based Verification system has been challenged by sophisticated attacks, the new advanced schemes are being made to cover the weakness of the password-based systems. However, the identification part is still done based on a public login ID. We proposed a new scheme called mind metrics to strengthen the identification process with personal secret information.

Acknowledgement

The authors would like to thank the supports given by the Vignan's University in terms of financial and technical supervision.

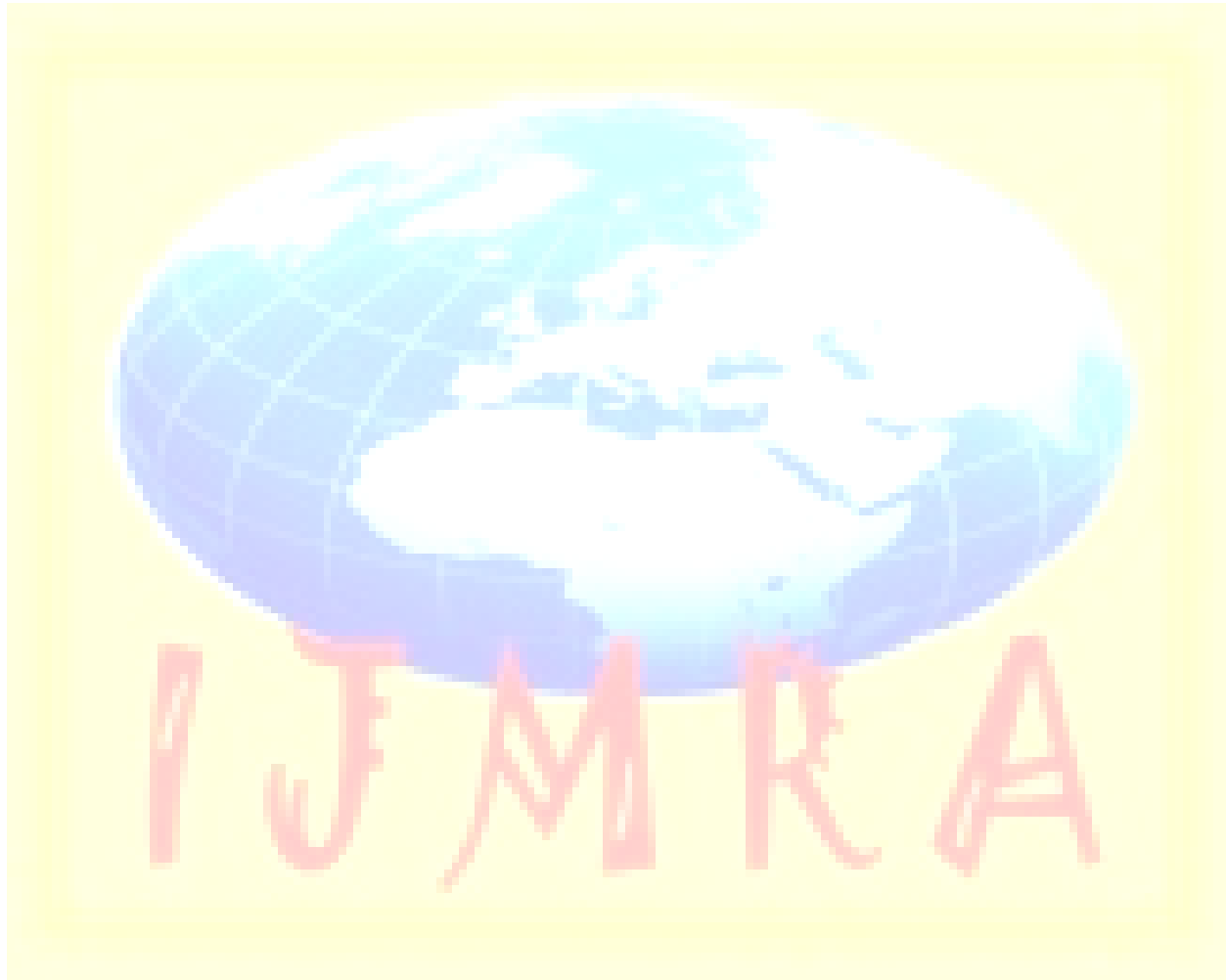
References

The main references are international journals and proceedings. All references should be to the most pertinent and up-to-date sources. References are written in Vancouver style. Please use a consistent format for references – see examples below



- [1] Anna Vapen, David Byers, and NahidShahmehri, "2-clickAuth –Optical Challenge-Response Authentication", 2010 International Conference on Availability, Reliability and Security, pp. 79 – 86
- [2] AlonSchclar, LiorRokach, Adi Abramson, and Yuval Elovici, "User Authentication Based on Representative Users", IEEE Transactions On Systems, Man, And Cybernetics—Part C: Applications And Reviews, Vol. 42, No. 6, November 2012, pp. 1669 – 1678
- [3] Bin B. Zhu, Jeff Yan, Guano Boa, Maowei Yang, and NingXu,"Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems", IEEE Transactions on Information Forensics And Security, Vol. 9, No. 6, June 2014, pp. 891 – 904
- [4] Bob Zhang, Wei Li, Pei Qing, and David Zhang, "Palm-Print Classification by Global Features", Ieee Transactions On Systems, Man, And Cybernetics: Systems, Vol. 43, No. 2, March 2013, pp. 370 – 378

- [5] Chao Shen, ZhongminCai, Xiaohong Guan, Youtian Du, and Roy A.Maxion, "User Authentication Through Mouse Dynamics", IEEE Trans on Information Forensics and Security, v. 8, no. 1, Jan 2013, pp. 16 – 30
- [6] Dileep Kumar, YeonseungRyu, and Dongseop Kwon, "A Survey on Biometric Fingerprints: The Cardless Payment System" 2008 Int'l Symposium on Biometrics and Security Technologies, pp. 1-6
- [7] Emmanouil Georg kakis, Nikos Komninos, Christos Douligeris, "NAVI: Novel Authentication with Visual Information", IEEE Symposium on Computers and Communications, 2012 , pp. 588 – 595
- [8] Feng Zhang, A. Kondoro and S. Muftic, "Location-Based Authentication and Authorization Using Smart Phones", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2012, pp. 1285-1292
- [9] JožeGuna, IztokHumar, and MatevžPogajnik, "Intuitive Gesture Based User Identification System", 35th International Conference on Telecommunications and Signal Processing (TSP), 2012, pp. 629 – 633
- [10] Joseph Bonneau, Cormac Harley, Paul C van Outshot, and FrankStajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes", 2012 IEEE Symposium on Security and Privacy, pp. 553 – 567
- [11] Jaeseok Yun, Gregory Abowd, Woontack Woo, JehaRyu, "Biometric User Identification with Dynamic Footprint", 2007, 2nd Int'l Conference on Bio-Inspired Computing: Theories and Applications, pp. 225-230
- [12] M. Alzomai, A. Jøsang, A. McCullagh, E. Foo, "Strengthening SMSBased Authentication through Usability", International Sump on Parallel and Distributed Processing with Applications, 2008, pp. 683 – 688
- [13] Mariusz Rybnik, MarekTabedzki, and Khalid Saeed, "A Key stroke dynamics based system for user identification, 7th Computer Information Systems and Industrial management Applications, 2008 pp. 225 – 230
- [14] N. Sklavos and C. Efstathiou, "SecurID Authenticator: On the Hardware Implementation Efficiency", 14th IEEE International Conference on Electronics, Circuits and Systems, 2007, pp. 589 – 592

- [15] Ponemon Institute Research Report, “2013 Cost of Data Breach Study:Global Analysis”,day2013,availableonhttps://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WPPonemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf
- [16] Zahid Syed, Sean Banerjee, Qi Cheng, BojanCukic, “Effects of user habituation in keystroke dynamics on password security policy, 2011 IEEE 13th International Symposium on High-Assurance Systems Engineering, pp. 352 – 359



BIBLIOGRAPHY OF AUTHORS

	<p>VANITHA LAM,pursuing the post-graduation degree in master of technology in Electronics and communication engineering from the Lingaya’s Institute of Management and Technology, Krishna district, Andhra Pradesh, India.</p>
	<p>VenkatraoTadiseti, Currently, he is the Asst.professor in the department of Electronics and communications in Lingaya’s Institute of Management and Technology.</p>

