International Journal of Scientific Research in Computer Science and Engineering
Vol.6, Issue.1, pp.44-49, Feb (2018)

Research Paper

E-ISSN: 2320-7639

GSM devices Property proof and Tracking

Hussam Elbehiery

Department of Computer Networks, Ahram Canadian University (ACU), Giza, Egypt

**Corresponding Author: hussam.elbehiery@gmail.com, Tel.: +201027199717*

Available online at: www.isroset.org

Received 29/Jan/2018, Revised 05/Feb/2018, Accepted 18/Feb/2018, Online 28/Feb/2018

***Abstract*—** All GSM network devices such as smart phones become a target of choice for thieves because they are small, valuable, and there is a market for them. A thief can sell a stolen electronic device to an unsuspecting used computer store or pawnshop, and easily receive up to half its value in cash. The penalties for a property crime are less severe than those of a crime against a person is another reason of wide spreading of this crimes. Cost of this crimes is not just its replacement cost, but also the cost of configuring and loading replacement software, and the cost of lost time for the owner while the device is being replaced. An even greater cost is the potential exposure and liability that results from lost confidential corporate and client information. Designed web page will be used to access these devices to take always a copy of the important data and will be saved on the cloud area related to the web site which make it easier to retrieve the stored information in theft or lost case. The introduced research explains how you can keep strangers from accessing your personal information, safely back up and retrieve the stored data in the device. The introduced design will help in trying of minimization of the theft cases also minimizing extortion by thieves or some of exploiters depending on that all GSM device especially cellular phones could be tracked using IMEI (International Mobile Station Equipment Identity) or MEID (Mobile Equipment Identifier).

***Keywords*—** Cellphone tracking, Property Proof, and Data Retrieval

I. Introduction

Unsurprisingly, the thefts grew most rapidly in urban areas where cell phone density is highest. So they think firstly in stored data on these devices as the world become live in the digital life. However, because of their portability, mobile devices are more susceptible than desktop systems to loss and theft. Safeguards you can use to reduce the risk of someone accessing personal and institutional data when your mobile device is lost or stolen [1].

First of all some security features on smartphones which are using the GSM services should be enabled which is also vary between devices and operating systems (iOS, BlackBerry, Android, Windows Phone, and Windows Mobile) to configure security and encryption settings. [2] Use whichever features your device offers that provide the best security for your needs such as: Password, passcode, or PIN, Unlock pattern, Device lockout, Auto-wipe, and Encryption.

The following common features are frequently useful, but can also create security risks [3]. You may want to consider disabling them: Bluetooth, and GPS.

The suggested system depend on developing a web application system to verify an ownership for the customer's cellular phones and the GSM devices. There will be an employees who are responsible for client registration on the tracking and protection site in addition to the possibility of changing the ownership from the original client to any another customer (who the original client could choose) and the normal inheritance operations (son, daughter, brother, sister, relatives, etc.). In case of theft, the customer can contact the responsible employee in the suggested system or go to nearest branch to complete or finalize any operation related to this issue. Customer can see all the purchases of cell phones or GSM devices directly through the system website and all of the auxiliaries' customers [5,11].

There are specific websites are available for both iOS and Android devices and combines security, tracking, and anti-virus/malware protection. There are several interesting features, such as the system recording a cell phone's last location right before the battery dies, a chance to backup contact data before a remote erase, and it'll even snap a photo of any would-be thief and email it along with location data to you. There's a free two-week trial, after which it'll cost $5 per month approximately [6,9,10].

The rest of the paper is organized as follows: Section 2 highlights the system analysis and design for the proposed work whereas the web application output framework is explained in Section 3. The MD5 (Message-Digest) encryption algorithm is explained in Section 4. The Authorization (Permissions) and recovering lost data are stated in Section 5 and Sections 6. The Insurance and Tracking methodology are discussed in Section 7. Finally, the conclusion of this research work are elucidated in the section 8.

II. SYSTEM ANALYSIS AND DESIGN

Cellular phones have a unique serial number known as an IMEI (International Mobile Station Equipment Identity) or MEID (Mobile Equipment Identifier). Unlike other identifying information stored on the phone’s removable SIM card, these numbers are etched into its circuits and difficult to alter. Your cell carrier already has this 15-digit number on file, and may be able to use it to put the phone on a missing phone list. Some police departments ask for either of these numbers when you report a stolen phone, so that they'll be able to return it to you if it's recovered. You can typically find either number on the phone box or in your phone's settings menu. It is also often found printed on or under the phone’s battery. You can find your phone's IMEI by dialing *#06#. The number should pop up on your screen [7,18].

You'll find an IMEI number on all phones from GSM carriers such as AT&T and T-Mobile, and so-called world phones from CDMA carriers such as Verizon and Sprint. Less-common non-world phones from Verizon and Sprint have a different ID number called a mobile equipment identifier, or MEID. The MEID is comparable; you can find it the same way you find an IMEI. [8,19].

The suggested web application system is not only just a program but also all associated documents and configuration data which is needed to implement the suggested system. The first step is data base as following:

A. Database structural design

This logical data model contains all the needed logical and physical design choices and physical storage parameters needed to generate a design in a data definition language, which can then be used to create a database. Fig. 1. Shows the overall Use Case Diagram for the suggested systems and Fig. 2. Shows a schema that describe fully attributed data model contains detailed attributes for each entity [4].

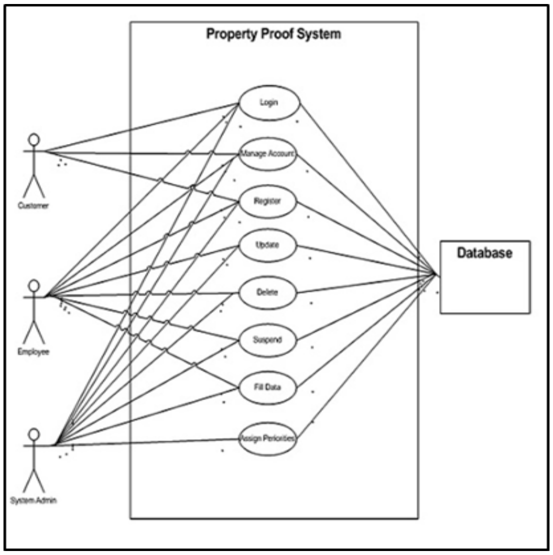


Figure 1. Use Case diagram for the suggested design

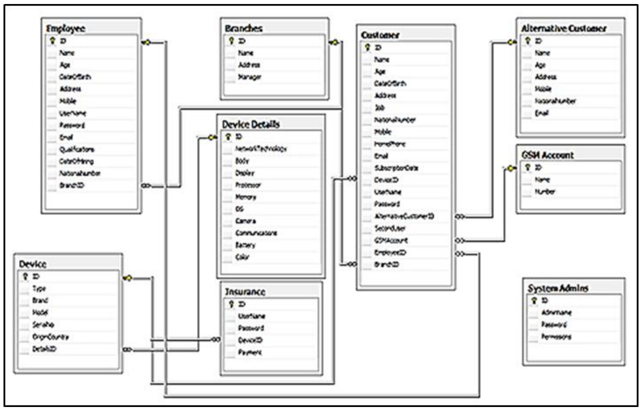


Figure 2. Database schema (Structural design)

In the suggested system we can send and retrieve the information directly through web application system to the internal DB including all permissions and encryptions. Various software have been used in that purpose like: XAMPP server, PHP frame work [4].

Unless you are running a live web server, you won’t need anything beyond Apache, MySQL and PHP, although it is a good practice to install all other components as well. You also have the option of installing a smaller ‘*XAMPP Portable Lite*’ version, which only includes essential *Apache, MySQL, PHP* and *phpMyAdmin* components.

III. WEB APPLICATION OUTPUT FRAME WORK

The first interaction process in the web application is the (*Add or insert process*) which will be seen in Fig. 3. This operation basically is stored in our SQL server database exactly in (System Admins) table the internal insert code in the database is performed in a query as the following [20].

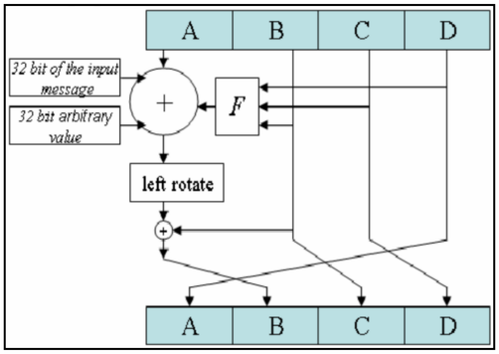
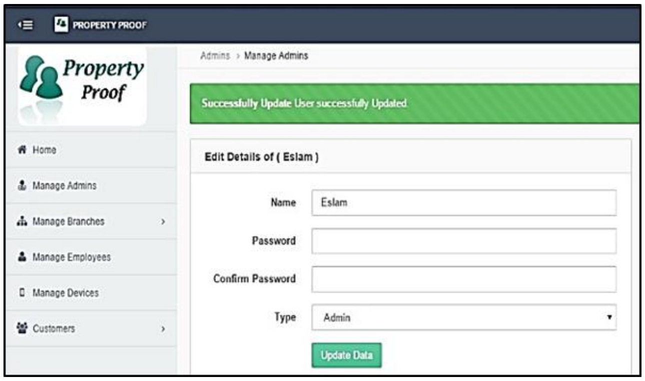


Figure 3. Add or Insert Process

The second interaction process is the update process which includes the editing of each information for the admin of the web application has been shown in fig. 4. This process implemented in SQL server database.



Successfully Update User successfully Updated

Edit Details of (Eslam)

Name: Eslam

Password:

Confirm Password:

Type: Admin

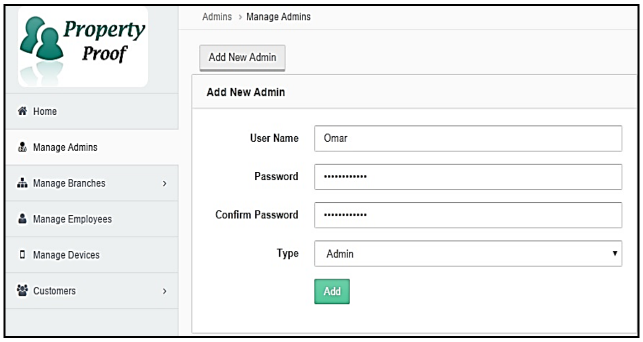
Figure 4. The update process

The third interaction (delete process) which includes the deleting for any admin and it is as the same in either first or second interaction processes implemented in SQL server.

IV. MD5 (MESSAGE-DIGEST) ENCRYPTION ALGORITHM

Now let's talk about how we can encrypt the most important data such as the "password". It is a widely used encryption hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been used in a wide variety of encrypt applications, and is also commonly used to verify data integrity.MD5 was designed by Ronald Rivst in 1991 to replace an earlier hash function, MD4 source code [13,14,15].

The main MD5 algorithm operates on a 128-bit, divided into four 32-bit words, denoted A, B, C, and D. These are initialized to certain fixed constants. The main algorithm then uses each 512-bit message block in turn to modify the desired word in a specific way. And return it in the same way [16,17]. Fig. 5. Shows the MD5 algorithm chart.



Add New Admin

User Name: Omar

Password: ············

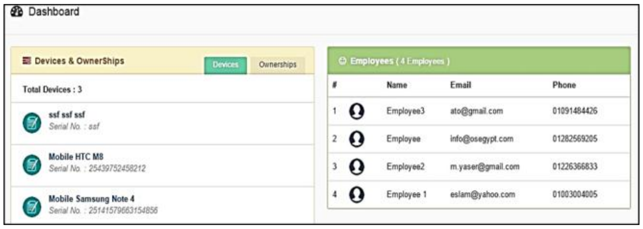
Confirm Password: ············

Type: Admin

Figure 5. MD5 algorithm

V. AUTHORIZATION (PERMISSIONS)

In multi-user computer systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use (such as access to which process he should reach, and can't reach other processes he doesn't get permission on it. Assuming that someone has logged in to a computer operating system or application, the system or application may want to identify what resources the user can be given during this session. Thus, authorization is sometimes seen as both the preliminary setting up of permissions by a system administrator and the actual checking of the permission values that have been set up when a user is getting access. Fig. 6. Shows the admin authorities and terms of reference, so the admin become able to manage every things in the whole system.



Total Devices : 3

ssf ssf ssf
Serial No. : ssf

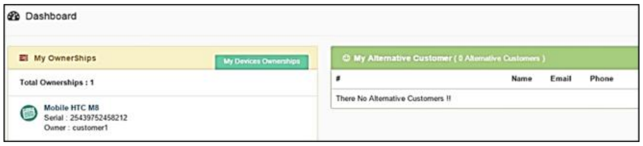
Mobile HTC M8
Serial No. : 25439752458212

Mobile Samsung Note 4
Serial No. : 25141579663154856

#	Name	Email	Phone
1	Employee3	ato@gmail.com	01091484426
2	Employee	info@osegypt.com	01282569205
3	Employee2	m.yaser@gmail.com	01226366833
4	Employee 1	eslam@yahoo.com	01003004005

Figure 6. Admin GUI

In contrast to the customer, only can see his devices also the alternative customer and the customer does not have a permission to do anything except in case by the employee. Explained in Fig. 7, the customer GUI for using his/her information and ability for editing. The customer can't see or handle anything except his devices and his alternative in case they exist.



Dashboard

My OwnerShips

Total Ownerships : 1

Mobile HTC M8
Serial : 25439752458212
Owner : customer1

My Alternative Customer (0 Alternative Customers)

#	Name	Email	Phone
There No Alternative Customers !!			

Figure 7. Customer GUI

VI. RECOVERING LOST DATA

As the device stores tons of important data on it, it may annoy you so much if you lose your files on your device suddenly. For instance, you may delete the photos, contacts, text messages and so on by accident. When you want the important data back, you find it really difficult to find a good method that can recover in a simple way. If you have the backup copies of the media files such as photos, audios, videos and so on, you are able to restore them easily to your phone. So in the introduced system as your phone become has an account and authorization permission, all you need to do is to connect your device to customer screen and share all data stored on phone in a cloud area for each user. All user have a choice that the sharing being manually or automatic which is making the restoring or retrieving the data from the lost phone is a simple operation.

VII. INSURANCE AND TRACKING METHODOLOGY

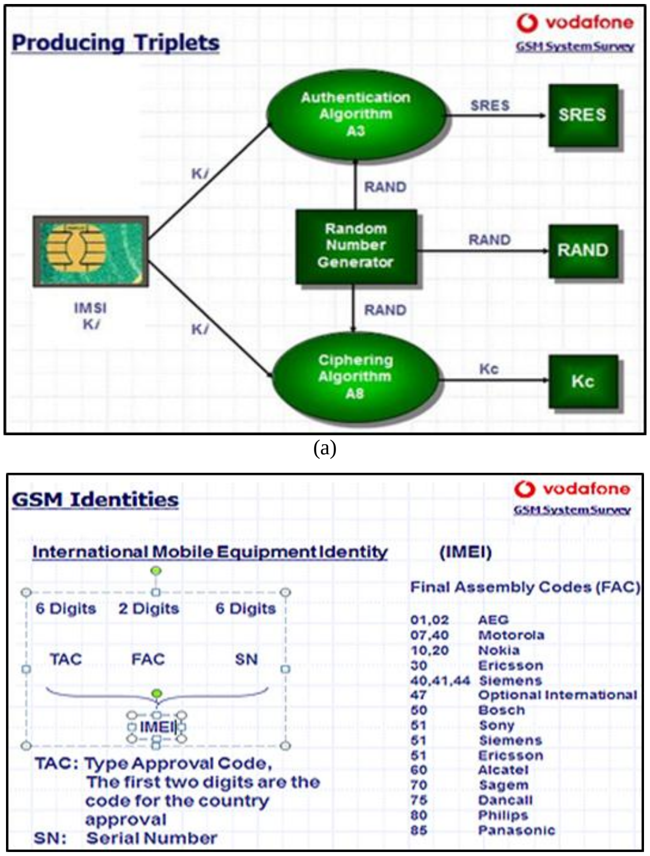
Insurance involves pooling funds from many insured entities (known as exposures) to pay for the losses that some may incur. The insured entities are therefore protected from risk for a fee. When a customer lose or got his phone robbed or Brocken and this phone can't be regained by our system then we must have plan B works for emigrant cases that we save what we can save. If the phone is damaged by the customer in this case we are not responsible for the maintenance as any insurance operation.

A customer who want to insure his phone he choose a plan of insurance of our plans and pay insurance quota and enjoy our insurance service. Note that the introduced system insure only the phone not the data inside. If you fall in one of these dangers (Accidental Damage – Loss - Theft) you will be covered by the insurance unless we cannot track your phone in case if it got lost. When the cell phone is got lost there are two ways and in both ways we must follow the official procedures; The Governmental method and the Software application method.

To inform the office of communication police office with an official police report and have an official copy of it to inform all cell phone carriers to flag your phone, which will be done through the next steps:

- When you report the police you give them the property proof only (receipt or the phone package) your phone and they take also the (IMEI) every mobile phone, GSM device or other devices with a built-in phone / modem has a unique 15 digit IMEI number. Based on this number, you can check some information about the device.
- The second step is to inform the GSM operators to block or locate your mobile phone to enable the police to get it back.

If you have lost your mobile phone or if it's stolen, then you can recover it or at least block it if you know the IMEI number of the phone. The procedure to get back the stolen mobile phone will take some time so you must be patient. Fig. 8 (a) shows the GSM network basic structure (Vodafone) and Fig. 8 (b) shows the GSM network identities (Vodafone).



Producing Triplets

(a)

GSM Identities

International Mobile Equipment Identity (IMEI)

TAC: Type Approval Code,
The first two digits are the code for the country approval
SN: Serial Number

Final Assembly Codes (FAC)

01,02	AEG
07,40	Motorola
10,20	Nokia
30	Ericsson
40,41,44	Siemens
47	Optional International
50	Bosch
51	Sony
51	Siemens
51	Ericsson
60	Alcatel
70	Sagem
75	Dancall
80	Philips
85	Panasonic

(b)

Figure 8. a) Basic GSM Network Structure b) GSM Identities

There are some specific apps that help in tracking lost or stolen cell phones. For example, check the Bitdefender for all cell phones or any GSM devices. It is available for the *iOS* operating systems (iPhone) and *Android* operating systems [12]. Then follow the next steps:

- Download the registered Bitdefender application to your device.
- Register to the site https://my.bitdefender.com/login and then login to the created account.
- Select the feature you want to use; (locate- lock – alert- wipe) or Anti-Theft.

VIII. CONCLUSION

The introduced research paper is a web application system which has been developed for the purposes of protection of the cell phones or any GSM devices and also keeping all information which takes higher priority of privacy for these devices. The proposed research has explained keeping strangers from accessing the personal information, safely back up and retrieve the stored data in the device. The major usefulness is to verify an ownership for the customer's devices especially in case of purchase from customer to customer with no needed to the package box or the original receipt which will verify the concept of Property Proof.

ACKNOWLEDGEMENT

This research was supported by **Ahram Canadian University**. I would thank my colleagues from **Faculty of Computer Science and Information Technology** who provided insight and expertise that greatly assisted the research.

REFERENCES

[1] Josh Lockhart, "Modern PHP: New Features and Good Practices Paperback, " laxmi publications, USA, 2015.

[2] W. Stallings, "Data and Computer Communications," ©2007 Pearson Education, Inc. Pearson Prentice Hall Pearson Education, Inc. Upper Saddle River, NJ 07458, 8th Edition, ISBN: 0-13-243310-9, USA, 2007.

[3] Michael Hogan, Fang Liu, Annie Sokol, and Jin Tong, "NIST-SP 500-291, NIST Cloud Computing Standards Roadmap," National Institute of Standards and Technology Special Publication 500-291 V2, Spec. Publ. 500-291, 108 pages, NIST Cloud Computing Program Information Technology Laboratory, USA, 2013.

[4] Sikha Bagui and Richard Earp, "Database Design Using Entity Relationship Diagrams," AUERBACH PUBLICATIONS, A CRC Press Company Library of Congress Cataloging-in-Publication Data ISBN:0849315484, UK, 2011.

[5] U. S. Pandey and Rahul Srivastava, "E- Commerce and Mobile Commerce Technologies," S. Chand Publisher, Vedams eBooks (P) Ltd., ISBN 10: 8121928419 / ISBN 13: 9788121928410, New- Delhi, India, 2007.

[6] Mathew Johnson, "A New Approach to Internet banking," Technical Report, UCAM-CL-TR-731, University of Cambridge Computer Laboratory, ISSN 1476-2986, UK, 2008.

[7] N. H. MohdAlwi and I.S. Fan, "Information security threats analysis fore-learning," *Proc. 1st Inter. Conf. of TECH-EDUCATION, CCIS*, vol. 73, pp. 285-291, Athens, Greece, 2010.

[8] A. Kapil and A. Garg, "Secure web access model for sensitive data, "International Journal of Computer Science & Communication (IJCSC),vol. 1, no. 1, pp. 13-16, India, 2010.

[9] Michael E. Whitman, and Herbert J. Mattord, "Principles of Information Security," 4th Edition, CENAGE Learning, ISBN-13: 978-1-111-13821-9, ISBN-10: 1-111-13821-4, Nelson Education Ltd., USA, 2012.

[10] Melchor, C.A., and Gaborit, "A fast private information retrieval protocol," In ISIT 2008. pp. 1848 – 1852. IEEE, 2008.

[11] Ostrovsky, R., Skeith, and W.E., "A Survey of Single-Database Private Information Retrieval: Techniques and Applications," In Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp.393–411. Springer, 2007.

[12] Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat,
Harri Hursti, Margaret MacAlpine, and J. Alex Halderman, "Security Analysis of the Estonian Internet Voting System," CCS '14 Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security Pages 703-715, ISBN: 978-1-4503-2957-6, Scottsdale, Arizona, USA, 2014.

[13] V. Ciriani, S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Combining fragmentation and encryption to protect privacy in data storage," ACM Transactions on Information and System Security(TISSEC), vol. 13, no. 3, New York, USA, 2010.

[14] Baek, J., Susilo, W., and Zhou, J., "New constructions of fuzzy identity-based encryption," In ASIACCS 2007, pp. 368–370. ACM, Singapore, 2007.

[15] Zhou, Jianying, Young, Moti, Bao, and Feng (Eds.), "Applied Cryptography and Network Security," 4th International Conference, ACNS 2006, Singapore, June 6-9, 2006, Proceedings, ISBN 978-3-540-34704-0, Springer Publishing, USA, 2006.

[16] Vitaly Dubravin, "Is Data Masking better than Encryption," Droid Cafe; Life in Technology, 2011.

[17] Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman, "An Introduction to Mathematical Cryptography," Springer Science and Business Media, LLC, ISBN 978-1-4939-1711-2, 2nd edition, XVII, 538 p. 32 illus., USA, 2014.

[18] Siddharth Agarwal, AbhinavRungta, R.Padmavathy, Mayank Shankar and NipunRajan, "An Improved Fast and Secure Hash Algorithm," Journal of Information Processing Systems, Volume 8, No.1, ISSN: 2092-805X, Korea, 2012.

[19] Nabil H. Shaker, Hanady H. Issa, Khaled A. Shehata and Somaia N. Hashem, "Design of F8 Encryption Algorithm Based on Customized Kasumi Block Cipher," International Journal of Computer and Communication Engineering, Volume 2, No. 4, ISSN: 2010-3743, International Academy Publishing (IAP), USA, 2013.

[20] Jon Duckett, "HTML and CSS: Design and Build Websites," John Wiley & Sons, Inc., Indianapolis, 1st Edition, ISBN: 978-1-118-00818-8, Indiana, USA, 2011.

[21] Chen, T.H., Hsiang, H.C. and Shih, W.K., "Security improvement on a remote user authentication scheme using smart cards," 4thInternational Conference of Information Security and Assurance, Communications in Computer and Information Science, Vol. 76,pp.9–16, Japan, 2010.

[22] Debiao, H., Jianhua, C. and Jin, H.,"Weaknesses of a

dynamic ID-based remote user authentication scheme," International Journal of Electronic Security and Digital Forensics, Vol. 3, No. 4, pp.355–362, USA, 2010.

[23] Khan, M.K., Kim, S.K. and Alghathbar, K., "Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme'," Journal Computer Communications, Vol. 34, No. 3, pp.305–309, ISSN: 0140-3664, Elsevier Science Publishers B. V. Amsterdam, The Netherlands, 2011.

[24] Wang, Y.Y., Kiu, J.Y., Xiao, F.X. and Dan, J.,"A more efficient and secure dynamic ID-based remote user authentication scheme," Computer Communications, Vol. 32, No. 4, pp.583–585, ISSN:0140-3664, Elsevier Science Publishers B. V. Amsterdam, The Netherlands, 2009.

[25] B.G. Nagaraja, Ravi Rayappa, M. Mahesh, Chandrasekhar M. Patil, and Dr. T.C. Manjunath, "Design & Development of a GSM Based Vehicle Theft Control System," 978-0-76953516-6/08©2008IEEE, DOI10.1109 / International Conference on Advanced Computer Control ICACC 2009, pp.148-152., Singapore, 2009.

[26] CCMTA, "Best Practice Models for Combating Auto Theft," Version 6.1, Anti Auto-Theft Project Group, Canada, 2006.

[27] EdigaLingappa, Geetavani.B, and JambulaHareesha, "Online Signature Verification using Dynamic Properties," International Journal of Scientific Research in Computer Science and Engineering (IJSRCSE), Vol.5, Issue.6, pp.33-38, India, 2017.

Authors Profile

Hussam Elbehiery received the B.Sc. degree in Communication and Electro-physics from the Faculty of Engineering, Alexandria University in 1994, He received the M.Sc. degree in Electronics from Benha University, Cairo, Egypt in 2001. He attained the Ph.D. in Electronics from Benha University in 2005. He took his Associate Professor degree in Computer Science field 2016. He was selected to Benha University as adjunct professor for teaching and graduation project's supervision. He has presided or participated in a variety of more than 40 graduation projects. He had chosen for supervision of many post-doctoral, PhD desertion and MSc thesis. He is currently working as the Head of Computer Networks Department – Faculty of Computer science and Information Technology – Ahram Canadian University. His current research interests include design and implementations of Biometric systems, embedded systems, ciphering algorithms, GPS applications, Computer Engineering applications and Wireless communication techniques.