

## Restricted Activation Via SMS For Mobile Contracting Service

Tara Nawzad Ahmad Al Attar<sup>1</sup>, Miran Hikmat Baban<sup>2</sup>

Computer Department, Sulamani University,  
KRG-IRAQ.

<sup>1</sup> taraattar@yahoo.com, <sup>2</sup> computer1science@yahoo.com

### ABSTRACT

*Before the Information and Communication Technology (ICT), the old traditional security was managed by human that is very easy to handle even inaccurate, expensive, and unreliable. Furthermore, it is very changeable from one person to another due to the human activity. Hence, the active person can work harder and better control than the passive person. The ICT modifies old fashion manual-security (MS) to modernize electronic security (ES). The ES has a significant role in modern society, for that reason, ES became a hottest topic in nowadays computer technology. Nevertheless, almost all members of the community own a mobile phone, that means if we wanted or not, the ICT sharing our life, and most of the Society members cannot cope without it. In this paper, we will find out better results of ES by combined two ICT components namely; (Clickatell) public network server and SMS-mobile communication public system over two different platforms such as the commercial Windows and open source Linux in the respects of better QoS (Quality of Service) and efficiency. Also, another aim is to test the effectiveness of the system over the mentioned operating systems.*

**Keywords:** E Security, Manual security, ICT, SMS, QoS, internet public network, E-Society

### INTRODUCTION

ICT: Any modifications occurred from past until now is called generation. Obviously, the modified toward to E-Society is a newer generation of computer science. The two generation technologies such as Clickatell and SMS with the encryption algorithm-security are combined and used for the reason of higher security and protection from any unauthorized attacks by users. The forgetful users can be protected by blended technology, the mean of blended that working simultaneously by SMS and Clickatell over Internet public network, in the respect of far from using of human influences.

Manual security requires much human power, papers, cost and time consumers and our proposed system helps to avoid all these mentioned faults. Due to the popularity of the new technologies it is very difficult to manage daily activity in our life without the mobile phone. The (SMS) is more reasonable and becomes very familiar if compared to other technologies (Bluetooth). This because all the other technologies create faults in the communication and very limited in distance and capacity [1]. Obviously, in our proposed system depends on utilizing of SMS- public network, and it returns to the unlimited service of the public network (SMS). The unlimited service means to unlimited participating of users and unlimited distance between mobiles. Also SMS is fully potable application in the mobile device.

Before Internet revolution, the regular mail (R-M) categories were in the traditional style or postal. Therefore, the performances, availability and quality of services (QoS) of (R-M) were in a tiny stage because the communication facilities were very primitive. However, the popularity of Mobile instrument-SMS and Internet service improve the style of life [2]. SMS stands for "Short Message Service" and uses mobile phones to transmit. SMS (or text

message) to and from mobile phones has grown into a highly popular technique of communication among society members [3]. The ICT modified all the traditional activity toward to online and mobile business, since that the organization has been changed from the traditional culture to the E-Society the security became harder to control than the traditional security. Even the traditional security was not that reliable and in a higher level of accuracy, but it was very easier to manage because of the limited human population and trusted of humans at that time.

From our experience with operating systems, Linux Operating system is much more secure than Window operating system. Some of these server programs have weakness that can allow outsiders to login to the system maybe be with root privileges. Luckily, Linux comes with some facility that we can use to make the internet service more secure [4].

Performance is an important aspect either in real life that is a traditional performance (TP) or virtually which is the world of technology. However, technology and performance together plays a significant role in real life [5]. The mobile -performance (M-Performance) is much better for the purpose of controlling security. Also, our proposed system has a significant role in solving real life problems, for example, those forgetful people and reminds them of the new password.

The role of clickatell is that to become a great backend and support the frontend of mobile technology by SMS through public network. Figure (1) shows the communication between client and server sides through SMS medium.

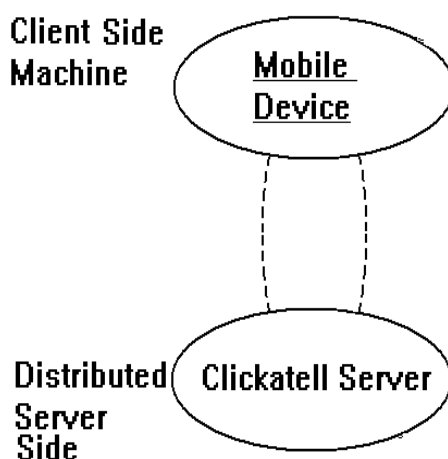


Figure 1. Communication through SMS for client and server sides

The Restricted Activation system took advantage of the international gateway namely Clickatell for the reason of reminding password by SMS. The contribution of our proposed system is to use the backend Clickatell application for the mentioned reason.

Clickatell is an international gateway that integrates and delivers SMS messages directly to mobile phones. It works over many networks in the countries all around the world. This gateway enables different groups for example, communities, governments, and institutions to use mobile messaging to help them with their businesses. It supports more than one connection method such as HTTP on port 80 and SMTP on port 25. It requires a clickatell account, PIN safe 3.x, and a mobile phone to receive the SMS text message [6, 7]. This is a great idea for providing users with a new password for those who have a problem with remembering their passwords

The used algorithm for the code encryption is by MD5 (Message-Digest) Hash Algorithm: The code that is sent to the verified phone number will be forwarded in an encrypted form until it reaches the user. MD5 is a popular encryption method that changes the readable password into unreadable text. This algorithm changes all passwords into 32 hexadecimal digits. It does not care how long the password is, and it'll become 32 hexadecimal digits. It produces a 128 bit (16 bytes) hash value, which is typically expressed in text format as a 32 digits hexadecimal number [8].

The proposed application namely restricted activation developed in PHP and MySQL by a ready software is XAMPP over different platform (OS), for example Linux and Windows. The performance of both platforms by developed and run identical applications. In both Operating Systems the Linux and Windows the measurement recorded as an execution time over both platforms. The paper starts with the background used for this research. Then, a brief description of the system as well as the trial that took place, subsequently a discussion of the survey results is present. Finally, the paper finished with a summary and conclusions.

## Background

Typically, users of a multiuser or securely protected single-user system claim a unique name (often called a *user ID*) that can be generally known. The term ID (which stands for Identification Device) is a unique name that is given to a user to gain access to a particular network, system, database, mailbox ...etc. It identifies the user to the system as an authorized user. It also called username. Usually, the ID is coupled with a password.

In order to verify that someone is entering that user ID really is that person, a second identification, the password, known only to that person and to the system itself, is entered by the user. Alternatively, we can say that the password is the security to prove that this user is the authorized person to whom that the user ID belong. A password is a sequence of characters (mix between letters, special characters and numbers) without spaces used to determine that a computer user requesting access to a computer system is really that particular user. A password is typically somewhere between four and 16 characters, depending on how the computer system is set up. When a password is entered, the computer system will not display the actual characters on the screen. Instead, it will show a sequence of black circles or stars. Thus, the next process will be done to protect the password from being seen by other persons sitting around the user.

## THE PROCESS OF RESETTING USER PASSWORD

This process involves three steps:

1. When a user first creates his account, the user will be forced to enter a valid phone number. Then can assume that this phone number is the criteria for resetting the password (Criteria creation cycle). It is important to define identification criteria that could be easily remembered and reproduced. Security Questions are not used here because there is an enormous chance that the user forgets the Question and/or the answer. On the other hand, cell phone numbers are something unforgettable. Therefore the user will be asked to enter a valid phone number. Entering this number is Mandatory, not an optional choice.
2. This step is used to establish the user identity when the user request for a password reset to verify the user (Verification Cycle). This cycle begins when a user completes all steps for creating a new account. Then the system must verify if the phone number entered by this user is really his own. If so, then the system will make

sure that this is a legitimate member of this system; otherwise he will deny access to the network with an alert. The phone verification is done by sending a code to it.

3. After the verification, the reset process will start by sending an SMS to the verified user with a code to reset his password (Resetting Cycle). When the user and his phone number are verified through the above process, an SMS will be sent to this phone number with a code. The user can use this code to gain access to his account, and once he logged into his account he will be forced to change his password to another one.

### Why Using ID and Password to Protect our System...

Using ID's and passwords has many advantages, first it is the cheapest method to use because it does not need any extra hardware or software installation. Plus the fact that it is easy to use by almost everyone. On the other hand, using this approach will have some disadvantages as well, first it is weak and can be easily attacked, the security level depend on the user himself and his ability to maintain the safety of his ID and password by choosing some complicated ones and changed them frequently. This approach is not advice for financial transaction at all.

### RESTRICTED ACTIVATION SYSTEM

The proposed system is a mobile contracting service system. Each has its own mobile device and whenever an individual wishes to view his mobile private information such as his balance, expiration date...etc. using this system, the user will be asked to enter own ID and password. Generally most of humans are forgettable creatures, so they can quickly forget their ID's and much easier their passwords! However, on the other hand, people do not forget their own phone numbers. Therefore, whenever a new user is signed into this system it will be asked to enter their phone numbers as a part of their sign in process.

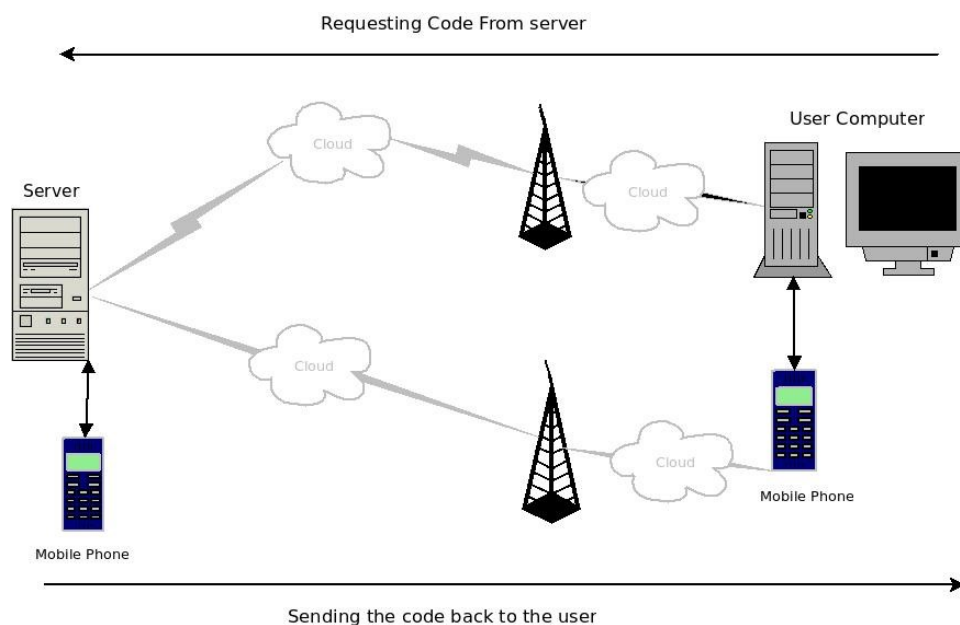


Figure 2. SMS-mobile and Clickatell

The users that not remember own password the system ask to enter own mobile number for the reason of verification between the entered phone number and phone number that was stored into the database of the system. The matchmaking is a suitable algorithm that used for better security level and verification. The user can get a new code for re-enter to the system and get new password in on choice. The enhanced matchmaking algorithm is that: If both

numbers are matched and same, the system will send a SMS message that contains a code. After the user entered the confirmed code to the system, the user will be forced to reset the password. Normally this is a way of getting new password and far from hacking the passwords. The two technologies SMS-mobile and Clickatell make us to be safe from hacking. Figure 2 shows the two technologies mentioned before.

Obviously the used network for our proposed system must be public network nor private network because of the limitation of public network are very wide and global but the private network limitation is local. As mentioned is restricted because of the new contribution in our proposed system if compared with others, the algorithm we used is resetting and get new password but the others enforce you double login. Of course the resetting password is much better and more secure than the double login. Figure (3) Shows the Restricted Activation System Flowchart. Figure (4) shows the Main screenshot of the Restricted Activation system Login.

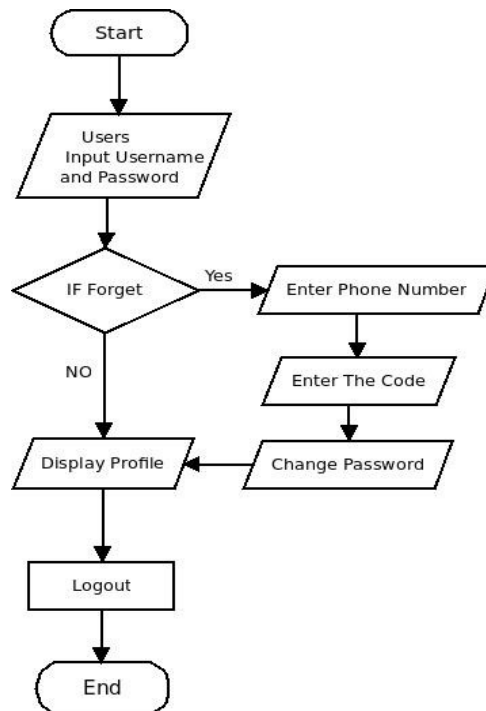


Figure 3. Restricted Activation System Flowchart

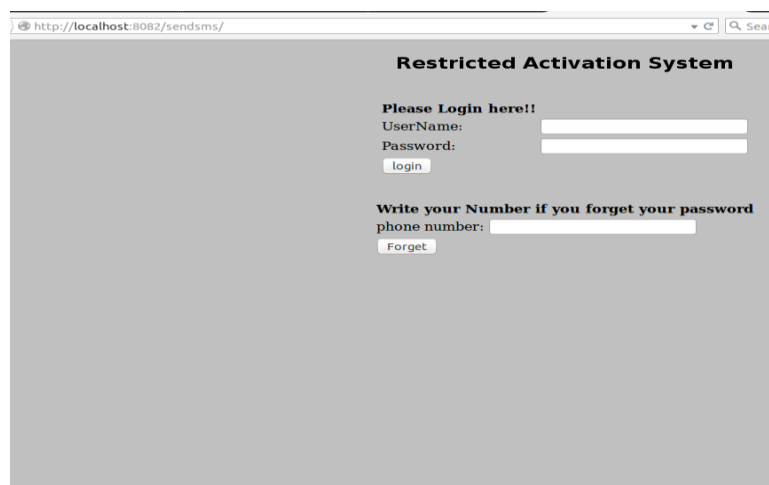


Figure 4. Main Restricted Activation System Screenshot

According to Figure (4) which is the main screenshot of the system and the system asked for username and password in order to let the user to log into the system. If the user remember the correct username and password then can access to the system Otherwise must be enter the previously verified phone number into the third combo box... After entering the mobile number, an SMS will be sent with a code to this user and this code will allow user to log into the system. Figure (5) show the successful login to the system but Figure (6) shows the unsuccessful access to the system and must get a code by SMS and enter to the system temporary for the reason of reset new password.

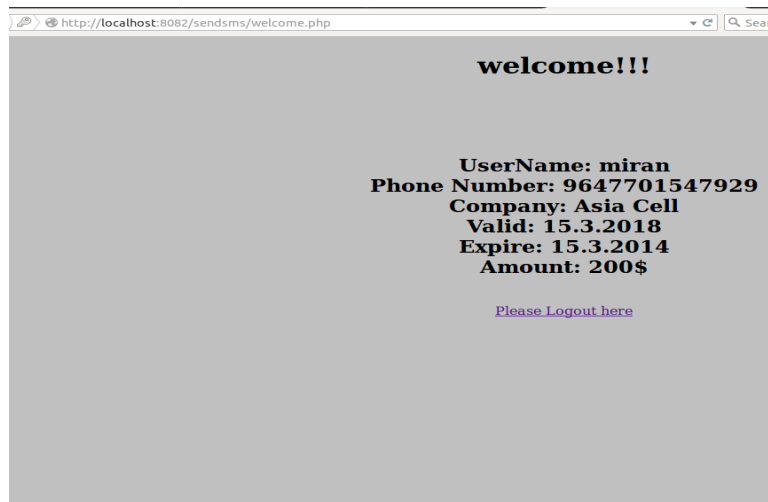


Figure 5. Successful login in Restricted Activation System Screenshot

As shown in Figure (5) all information are related to users in detail such as Username, phone number, mobile phone company name, the validation and expiration date of the mobile line and the amount of balance and log out bottom is available to log out of the system.

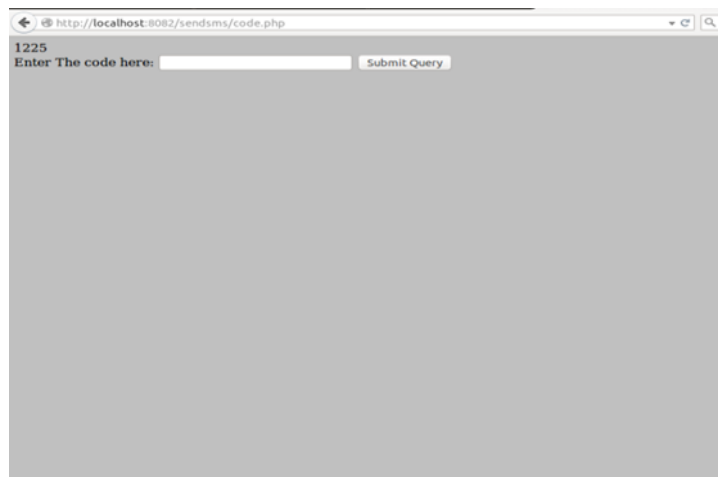


Figure 6. Unsuccessful login in Restricted Activation System Screenshot

The code sent by SMS let the user access to the system for only one time and get a new password. Figure (7) shows the enforce screenshot by system to user to reset password.



Figure 7. Enforce Restricted Activation System Screenshot

When user access to the system and rest password successfully the system let the password - forget user to login. Figure (8) let the user know that got new password and can login to the system.

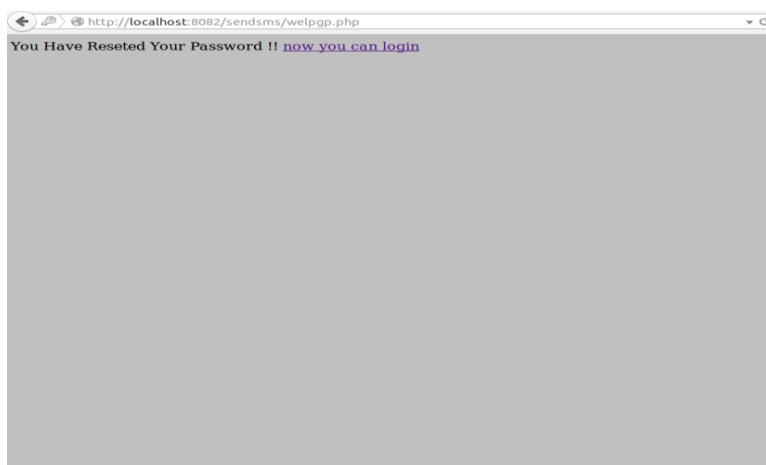


Figure 8. User acknowledgement regarding new password Screenshot

## SYSTEM REQUIREMENTS

### Software Specification

These software and applications have been used for designing the proposed system:

- Language: XAMPP
- Database: MYSQL
- Operating System: Linux (Ubuntu) and Windows (Windows 7).
- Application: Textpad

### Hardware Specification

The hardware that have been participated to propose our system:

**Desktop:** 4th Generation Intel® Core™ i7-4790 processor (8M Cache, up to 4.0 GHz), 8GB<sup>2</sup> Dual Channel DDR3 SDRAM at 1600MHz. NVIDIA GeForce GT 720 1GB DDR3. 1TB 7200 RPM SATA Hard Drive 6.0 GB/s.



**Laptop:** AMD Dual-Core E1-6010 Processor + AMD Radeon(TM) R2 Graphics. 4GB DDR3L System Memory (1Dimm).

**Smart Phone (Samsung 4S):** Android OS, v4.2.2 (Jelly Bean), v4.3, upgradable to v4.4.2 (KitKat), planned upgrade to v5.0 (Lollipop).

**Smart Phone (iPhone):** iOS, upgradable to iOS 4.2.1, 412 MHz ARM 11

**RESULTS AND DISCUSSION**

The system proposed and evaluated by two seminar-evaluations in the computer department, which took place in the main computer laboratory (LAB) at Sulamani University. We took advantage of using of three graduated students in case of testing the proposed system. However, the second seminar-evaluation took place in the main teaching association of the Sulamani University. The loading time and execution time of the system are tested over two different operating systems (OSs). The security as well as the loading time and execution time are main targets of our proposed system. The comparison result which are found out from the both evaluation test-one and test-two shows in Table (1) below. As we realized the total time (executing and loading) of Linux OS are much less than the total time (executing and loading) of Windows OS. A part of that the security level of Linux OS is higher that Windows OS. As mentioned before, Windows is commercial but Linux is open source.

**Table 1. Linux and Windows Execution Time and Loading time comparession**

No.	Operating System	Loading Time	Execution Time	Total
1	Linux	0.09 Second	0.05 Second	0.14 Second
2	Windows	0.12 Second	0.13 Second	0.25 Second

According to the table, the loading time is in seconds for each process, obviously the least loading time is good as performance but it’s not perfect as security level. The extra layers or tiers to create NTA for balance loading and better security, but time-loading is slightly higher. Figure (9) compares between the Execution time and Loading time of the Restricted Activation System when applied on two different OS Linux and Windows.



Figure 9. Execution time and Loading time Comparison



## **CONCLUSION**

Since another new modification introduced in the security by using of new technologies over two different Operating Systems with the use of public network. The Linux OS with public network namely mobile-SMS service has a great rule in society because it is much improved in the respect of Response time and loading time with better high level of security that showed in previous section results and discussion Table(1). Because of the high level of security Linux approved to use better than Windows and all results show our system is exactly support others previous works.

## REFERENCES

- [1] Kinsella, S. (2009). Many to one: Using the mobile phone to interact with large classes. *British Journal of Educational Technology*, 40(5).
- [2] Faraj, K. (2010). “Automated Recruitment System”, Faculty Science, Computer Department, University of Sulamani, KRG.
- [3] Faraj, K. A. A., & Najeb, A. A. (2013). “SMS-Classroom Feedback Systems”. *Tikrit Journal of Pure Science*, 18(3), 186-190.
- [4] Dulaney, E. (2010). “Linux for Dummies”. Etobicoke, ON: Willey publishing Inc.
- [5] Faraj, K. A. A., Ahmad, T. N., Mohammed, R. N., & Baban, M. H. M. (2013). “Web Technologies Performance Analysis for Different Platforms and Hardware Architecture”. *International Journal of Computer Networks and Wireless Communications (IJCNWC)*, 3(6), 449-455.
- [6] Clickatell Inc. (2015). Private Company Information. *Bloomberg Business week* 22 Oct 2015.
- [7] Clickatell Mobile Touch Multiplied. (2014). “Com API Specification V2.3.5”. Available at: [https://www.clickatell.com/downloads/com/Clickatell\\_COM.pdf](https://www.clickatell.com/downloads/com/Clickatell_COM.pdf)
- [8] Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2009). “Introduction to Algorithms” (3<sup>rd</sup> Edition). Cambridge, MA: MIT Press.