ISSN: 2321-7782 (Online)
Volume 2, Issue 2, February 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

CCT: An Efficient and Affordable User Authentication Protocol Defiant to Password Pinching and Reclaiming

M. Karthika[1]
M.E
Network Engineering
Francis Xavier Engineering College
Tirunelveli – India

Dr. R. Ravi[2]
M.E., Ph.D.
Professor & Head of CSE
Francis Xavier Engineering College
Tirunelveli – India

Abstract: ***Due to its convenience and ease of text secret code user Verification is the most popular form of websites. Users secret codes are stolen under a variety of threats and vulnerabilities are not compromised. First, users often choose weak secret codes and using secret codes across multiple websites again. Second, the threat of rogue thief suffers secret code, type the system secret code. Reusing a secret code, stealing a secret code to a user's cell phone and SMS service exists to thwart attacks, Cryptographic Cipher Text (CCT) Verification protocol design for a user name in which the cipher text is encoded and decoded by using hash function. In CCT each participating site has a unique telephone number, and registration is required and recovery phases, including a telecom service provider. The one-time secret codes in CCT are generated by secure hash function. The code i.e. secret code entered by the user will be encoded as plain text and decoded by the server as cipher text and delivered to the member's email-id as OTSC. For additional security the puzzle test will be conducted by the server to verify that either the user is an authenticated person or not. Through multiple hashing the set of one-time secret codes is established by a hash chain with the help of given input. By CCT, users only need not to remember any login secret codes. After CCT groundbreaking study, we compared CCT standard Web verification methods that are effective and affordable.***

Keywords: Cryptographic Cipher Text (CCT), OTSC (One-Time Secret Code), Click-Based Graphical Password (CBGP).

I. INTRODUCTION

The Secret code thief threats are caused by typing secret codes in to untrusted computers. An enhancement called Cryptographic Cipher Text (CCT), a user Verification protocol to protect user identity and access all websites; it proposes an extension of CCT. It requires for cell phone protection, account ID and secret code for a long term. A unique phone number for each participating site is required in CCT, and one- time secret code is required for registration and recovery phases, including a telecom service provider. User republishes SIM cards and enduring CCT system can recover secret codes. In comparison to conventional Web Verification methods CCT becomes more efficient and affordable.Cellphones and secret code to prevent secret code reclaim attacks till CCT SMS verification protocol proposed as a user name. Possesses a unique phone number for each website. The Listing and recuperation phases of a telecom service provider also participate. To reduce the pessimistic collision of human factors in the design of CCT as possible. By CCT, each user only has to protect his cell phone has been used, which have a enduring secret code. User be able to contact all websites are open from untrusted computers typing any secret codes. In comparison with previous projects, the first user Verification protocol named CCT protects from stealing the secret code (ie , phishing , key logger , and malware) attacks and prevent secret code reclaim. The advantage is that CCT ensures independence between each login. CCT to be fully functional, secret code recovery is considered and supported when users lose their phones. CCT prototype is implemented to measure its recital. The standard occasion used up on listing and login, respectively, 21.8 and 21.6 is s. As a result, the total execution time of the delay in SMS occupies more than 40 %. Using advanced devices can be short delay. Besides, CCT logon performance, for example, Pass faces is better than the graphical

© 2014, IJARCSMS All Rights Reserved

secret code schemes. Therefore, we believe CCT is accepted and trusted by users. Except for a few typing errors the login success time will be over 90 % .As a consequence , they all agreed Cryptographic Cipher Text (CCT) safer than the original login system . Of course, some of the participants want CCT original structure .CCT offers the following advantages.

1. Anti- malware (e.g., key logger) is surprisingly common, especially their secret codes, in which user gathers perceptive data. In CCT, users can log in to online services without entering secret codes on their computer. Therefore, a user secret code cannot get malware from untrusted computers.

2. Phishing fortification - ambassador to the users when they are laundered through fake websites and users launch phishing attacks to steal secret codes. As mentioned above, CCT allows users to successfully log into websites without revealing secret codes and computers. Users are guaranteed to withstand CCT phishing attacks.

3. Safe listing and Cryptographic Cipher Text (CCT) Recuperation – The SMS interface is an out-of- band communication. Get the right phone numbers, websites and users respectively. CCT uses a Telecom Service Provider (TSP), to collaborate. Establishing a secure channel recording and recuperation phases of the SMS aids message exchange in CCT. Designed to deal with cases like, when a user has lost his cell phone during the recovery phase. With the new SIM cards, CCT still works on the new handset.

4. Prevention of secret code reclaim and avoidance of weak secret code -CCT approach achieves one -time secret code. Vastly different secret codes are provided for each login to the cell phone. The login secret code is dissimilar for each other. Under this approach, users do not need any secret code to login. They put their phones to access the secret code for a long time, CCT work out the rest.

5. Cell Phone protection- An antagonist be able to whip users cell phones as well as attempt to go by all the way through user Verification .Conversely, the cell phones are secluded by an enduring secret code. The antagonist cannot imitate an authorized user to login devoid of being detected.

II. PREVIOUS WORK

Within the precedent little decades, the standard established as the major content secret code user confirmation on websites. Once registering an account on the website, public decides their username and secret codes in plain text. In order to effectively go into the website, users decide secret codes and the specified selected image to keep in mind .the user have to click five successive points on the specified image. In common, if users choose sturdy secret codes to secret code -based user verification be able to oppose brute-force and dictionary attacks to offer enough entropy .Conversely, secret code -based user verification content strings in the person mind experts is that there is a major trouble . This is referred to as the reclaim of the secret code. The unenthusiastic collision of the above troubles are caused by human factors .Consequently, when scheming a user Verification protocol must take into account human factors.

A. CBGP (Click-Based Graphical Password)

Click-based graphical passwords, which engross clicking a place of user-selected points, have been planned as a practical substitute to transcript secret codes. The crash on usability of a wide-range of descriptions, and collect in sequence concerning the point selected by users. CBGP test the users by three phases.

Each login starts by the following steps,

1. Construct Phase: Participants enter their username, selected a password by clicking five successive points on the specified image, and clicked on the Login button. Their password consisted of these five points in the particular order.

2. Authenticate Phase: The same image was accessible a second time and users be asked to verify their password. They formerly again entered their username and password then pressed the Login button.

© 2014, IJARCSMS All Rights Reserved

3. Login Phase: Participants then logged in using their previously created password.

III. PROPOSED SCHEME

In order to provide more security to secret codes than existing system, we are proposing a new technique known as OTSC on CCT protocol by using hash function i.e. one-time secret code for user verification on websites. Due to its convenience and ease of content secret code user verification is the most popular form of websites. However, user secret codes can be stolen by various threats and vulnerabilities and are prone to be compromise. Users frequently decide weak secret codes, and reclaim secret codes across multiple websites again. Typing secret codes into untrusted computers suffers secret code crook danger. The user verification protocol proposes the CCT enrichment to defend user identity; it requires a enduring secret code for cell phone fortification and account ID for login on all websites.CCT only requires every participating website possesses a exclusive phone number, and involves a telecom service provider in registration and recovery phases for the conception of one-time secret codes. In CCT there is no need of remembering the password for login; CCT automatically generates OTSC sequence for each login. User can recuperate CCT scheme with reissued SIM cards and enduring secret codes. CCT is proficient and inexpensive compared with the predictable web verification mechanisms.

A. One-Time Secret Code (OTSC)

The code i.e. secret code entered by the user will be encoded as plain text and decoded by the server as cipher text and delivered to the member's email-id as OTSC. For additional security the puzzle test will be conducted by the server to verify that either the user is an authenticated person or not.The one-time secret codes in CCT are generated by a protected one-way hash function. The set of one-time secret code is recognized by a hash sequence through several hashing, with a given input.

B. 3G link

User data and signaling data are used to prevent eavesdropping attacks and tampering attacks. 3G connectivity provides data confidentiality. Binary synchronous stream cipher and the confidentiality and integrity algorithms make a block cipher algorithm that is based on the algorithm F8 and F9 respectively. Users can firmly broadcast and obtain information to the web site through a 3G link.

C. Deployed Web Services

Deployed web services assist and enhance numerous applications like online banking, e-commerce, communal networks, and obscure computing. But user verification is merely handled by text secret codes for nearly all websites. There are several important disadvantages of applying text secret codes.

D. Modules Description

1) *Listing Segment:*

In the listing segment, user starts the CCT agenda to record latest account on the website to visit in the upcoming days. Unlike predictable listing, the server desires for the user's account credentials, as an alternative of secret code. Once satisfying out the listing form, the agenda asks the user to setup a master secret code. This master secret code is used to create a sequence of one-time secret codes for auxiliary logins on the target server. Then, the agenda routinely sends a listing SMS message to the server for finishing the listing process.

2) *Login Segment:*

Un-trusted browser sends a request to the server when the user starts the login phase. A method of user secret code, and the server is encrypted by means of an SMS message on his cell phone uses to provide the necessary information. Based on pre-shared secret document, the server can verify and authenticate the user on the grid shows information flows.

© 2014, IJARCSMS All Rights Reserved

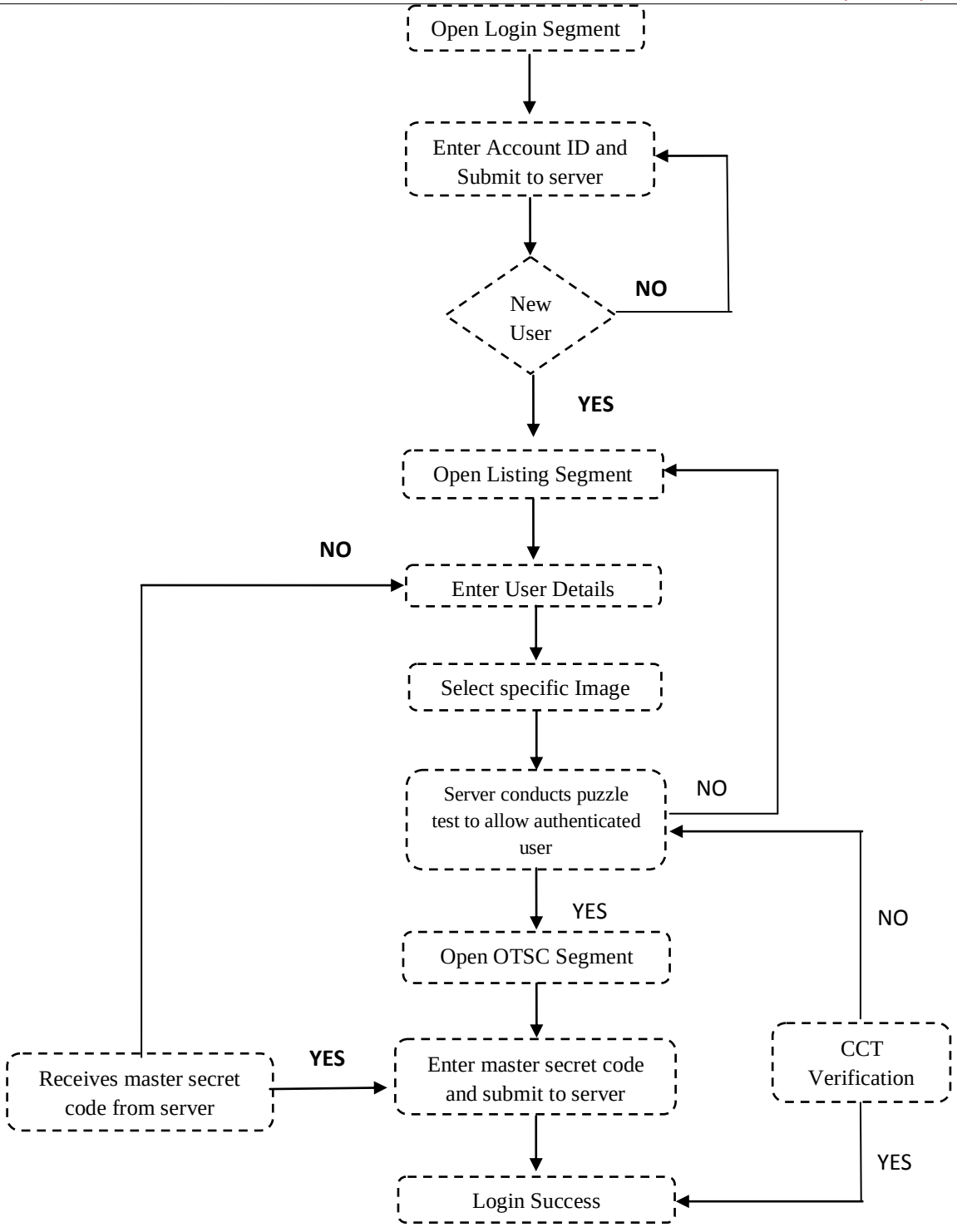


Fig 1: System Overview

3) *Image Selection Segment:*

After the login segment the users are allowed to select a specific image, in which he/she selects when listing her new account. This process is done to verify that the user is an authenticated person. If the use is an authenticated person then the user will be allowed to enter in to the website.

© 2014, IJARCSMS All Rights Reserved

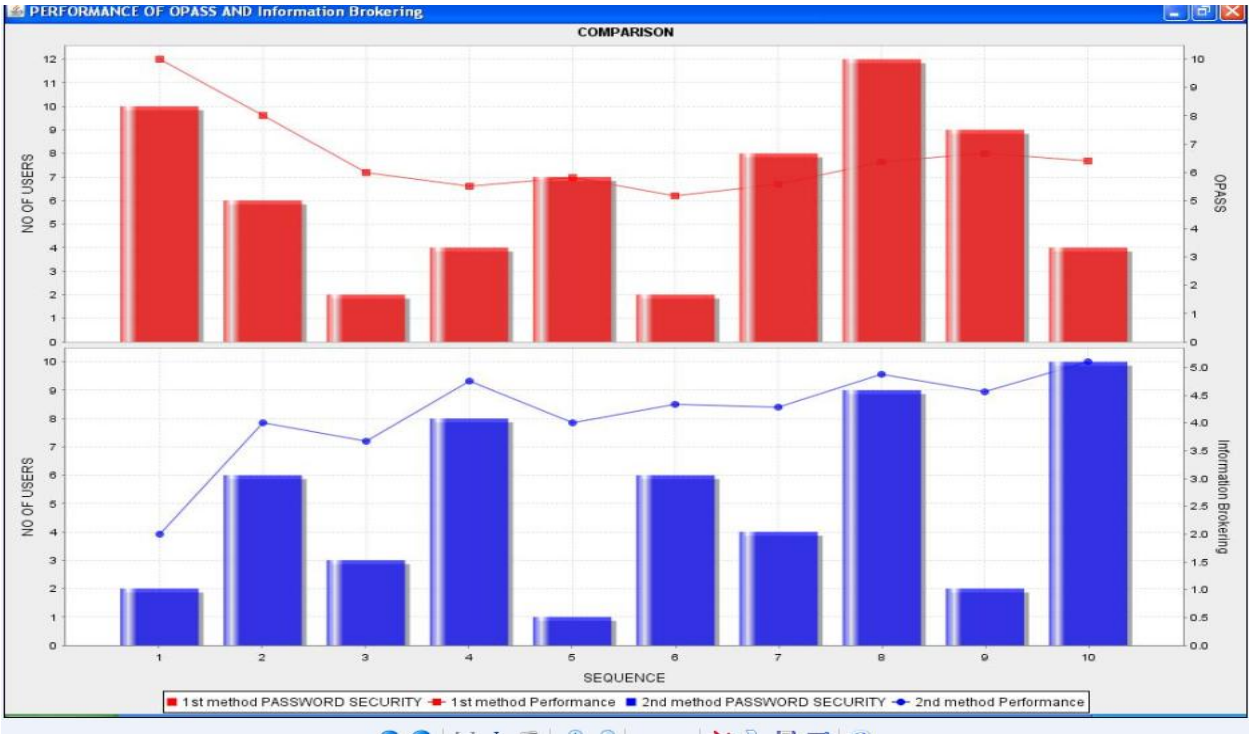
4) *Puzzle segment:*

In this segment the users are allowed to solve the puzzles to verify that they are authenticated. Users are allowed to finish a lot of the puzzles as probable in a specified period (about 3 minutes).If the user solves the puzzle then only the user is an authenticated user and the user is allowed to enter in to the OTSC segment.

4) *OTSC Segment:*

The Server produces the one time secret code (OTSC) and delivers via an Email to the user. The user opens Gmail and enters the OTSC number generated by server on the login page. The code i.e. secret code entered by the member will be encoded as plain text and decoded by the server as cipher text and delivered to the member's email-id as OTSC.

IV. RESULT ANALYSIS



A Defending user credential on ubiquitous web contact is essential because they are situated universally, such as airfield lounges, lodge commerce centers, and cafes. All sorts of attacks might occur in such settings, counting key logger, malware, and phishing. Consequently, we describe a risk replica of CCT and make obvious that CCT is protected later. In accumulation, we dissect CCT by a cryptographic procedure verifier. The hash sequence of a one-time secret code will be inspired completely. We set up restriction to resolve this trouble. The server checks the eminence of hash sequence subsequent to delivering a authorized login SMS. If the rest of the one-time secret codes are fewer than , the server sends a new kernel to the cellphone.Once the cell phone gets the new kernel, it computes the original license and sends it to the server through the SMS path. Consequently, the user and the server will utilize the original hash sequence for the subsequent login. This feature can be routinely finished devoid of user attempt. The out-of-sequence trouble is one more problem to the hash sequence. For illustration, the server's directory is i and the cell phone's directory is i+1 owing to several capricious errors. To tackle this trouble CCT adopts a fault-tolerant system. The server maintains a list of proceeding round OTSC δi while its directory moves to i+1. At the i+1th round, the server utilizes δi+1 to decrypt and confirm the legitimacy of the login SMS. If the confirmation is unsuccessful, the server checks the login SMS again by using δi .This system provides one fault-tolerant ability.CCT, requires a TSP (trusted proxy) to boost the safety. We assume this obligation is practical and not expensive since 3G telecom is broadly functional. Taking into account concert, the TSP is only concerned in the listing and revival phases. These two phases would be

© 2014, IJARCSMS All Rights Reserved

executed a little period for every exercise. In finale, CCT resists most attacks and has fewer desires than the previous systems. At last when compared to the existing systems CCT provides more security and performance.

V. CONCLUSION

The proposed system consist of a user verification procedure named Cryptographic Cipher Text (CCT) in which the cipher text is encoded and decoded by using hash function.CCT which leverages cell phones and SMS to frustrate secret code pinching and secret code reclaim attacks. Every website possesses a exclusive phone number. A telecom service provider participates in the listing and recuperation phases. The propose attitude of CCT is to eradicate the pessimistic authority of human factors as greatly as feasible. Through CCT, every user merely desires to keep in mind enduring secret codes which have been worn to defend her cell phone. Users are liberated from typing any secret codes into untrusted computers for login on all websites. Compared with preceding schemes, CCT is the original user verification protocol to avert secret code pilfering (i.e., phishing, key logger, and malware) and secret code reclaim attacks concurrently. The motive is that CCT adopts the one-time secret code loom to make sure liberty among every login. To make CCT entirely practical, secret code recuperation is also measured and supported while users mislay their cell phones. They can recuperate CCT scheme by means of reissued SIM cards and enduring secret codes. A sample CCT is also implemented to calculate its presentation. The typical moment used up on listing and login is 21.8 and 21.6 s, correspondingly. According to the consequence, SMS holdup occupies additional than 40% of whole implementation moment. The holdup might be shorter by means of higher procedure. In addition, the presentation of login of CCT is superior to graphical secret code schemes, for example, Pass faces. The login time of Pass faces is from 14 to 88 s, which is longer than CCT [48]. As a result, we consider CCT is tolerable and dependable for users. To scrutinize CCT usability, 24 participants are invited to conduct the user study. Most participants can simply activate all measures of the CCT scheme. The login sensation rate is above 90%, excepting for a little typing errors. Therefore, they all decided CCT is extra protected than the unique login scheme. Surely, some of the participants favor CCT to the unique scheme.

Acknowledgement

First of all we thank the almighty for giving us the knowledge and courage to complete the research work successfully. I express our gratitude to my respected Professor and Head of CSE Dr R.Ravi M.E.,Ph.D., for following me to do research work intentially.

References

1. Hung-Min Sun, Yao-Hsin Chen and Yue-Hsun Lin, 'oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks' IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.
2. B. Ives, K. R. Walsh, and H. Schneider, 'The domino effect of password reuse' Commun. ACM, vol. 47, no. 4, pp. 75–78, 2004.
3. S.Gawand and E.W.Felten, 'Password management strategies for online accounts' in SOUPS: Proc. 2nd Symp. Usable Privacy Security, New York, pp. 44–55, ACM,2006.
4. D. Florencio and C. Herley, 'A large-scale study of web password habits' in WWW: Proc. 16th Int. Conf. World Wide Web., New York, pp. 657–666, ACM 2007.
5. S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle, 'Multiple password interference in text passwords and click-based graphical passwords' in CCS : Proc. 16th ACM Conf. Computer Communications Security, New York, pp. 500–511, ACM 2009.
6. I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, 'The design and analysis of graphical passwords' in SSYM: Proc. 8th Conf. USENIX Security Symp., Berkeley, CA, pp. 1–1, USENIX Association 1999.
7. A. Perrig and D. Song, 'Hash visualization: A new technique to improve real-world security' in Proc. Int. Workshop Cryptographic Techniques E-Commerce, Cite seer, pp. 31–138, 1999.
8. J. Thorpe and P. van Oorschot, 'Towards secure design choices for implementing graphical Passwords' presented at the 20th. Annu. Computer Security Applicat. Conf., 2004.
9. S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, 'Passpoints: Design and longitudinal evaluation of a graphical password system' Int. J. Human-Computer Studies, vol. 63, no. 1–2, pp. 102–127, 2005.
10. S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, 'Design and evaluation of a shoulder-surfing resistant graphical password scheme' in AVI: Proc. Working Conf. Advanced Visual Interfaces ,New York, 2006, pp. 177–184, ACM,2006.

© 2014, IJARCSMS All Rights Reserved

11. C. Yue and H. Wang, 'SessionMagnifier: A simple approach to secure and convenient kiosk browsing' in Proc. 11th Int. Conf. Ubiquitous Computing, pp. 125–134, ACM,2009.
12. www.google.com

AUTHOR(S) PROFILE

M.Karthika is doing M.E Network Engineering in Francis Xavier Engineering College, Tirunelveli. She completed her B.E Information Technology in J.P. Engineering College, Agarakattu-Tenkasi in the year of 2012. She published many Conference Papers. She is an active member in Computer Society of India. Her areas of interest are Network Security, Wireless communication and Mobile Technology.

Dr. R. Ravi is an Editor in International Journal of Security and its Applications (South Korea). He is presently working as a Professor & Head and Research Centre Head, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli. He completed his B.E in Computer Science and Engineering from Thiagarajar College of engineering, Madurai in the year 1994 and M.E in Computer Science and Engineering from Jadavpur Government research University, Kolkatta. He has completed his Ph.D in Networks from Anna University Chennai. He has 18 years of experience in teaching as Professor and Head of department in various colleges. He published 12 International Journals, 1 National Journal. He is also a full time recognized guide for various Universities. Currently he is guiding 18 research scholars. His areas of interest are Virtual Private networks, Networks, Natural Language Processing and Cyber security.

© 2014, IJARCSMS All Rights Reserved