REFERENCES

A.Barth, Collin Jacjson and Jhon Mitchell (2008), "Robust Defences for Cross Site Request Forgery", ACM International Conference on Computer and Communications Security, pp:75-87, Virginia, USA.

Ahmed M. Elmisery, Huaiguo Fu (2010), "Privacy Preserving Distributed Learning Clustering of HealthCare Data Using Cryptography Protocols", 34th Annual IEEE Computer Software and Applications Conference Workshops, pp:140-145, Korea.

Alabrah and Mostafa (2012), "A Hierarchical Two tier one way Hash chain protocol for secure internet transactions", IEEE Global Communications Conference, pp:868-873, California.

Alex, Chin Huang and Mohamed (2007), "A Secure Cookie Protocol", IEEE Conference on Network Security", pp:333-338.

Alfaro and Novarro (2007), "Prevention of Cross Site Scripting attacks on current web applications", In On the Move to Meaningful Internet Systems, pp:1770-1784, Springer.

Angelo, Souto and Santos (2012), "Automatic Classification of Cross Site Scripting in web pages using document based and URL based features", IEEE Symposium on Computers and Communications, pp:702-707, Turkey.

Anthony.D.Miyazaki (2008), "Online Privacy and the Disclosure of Cookie Use : Effects on Consumer Trust and Anticipated Patronage", American Marketing Association, Vol:27, No:1, pp:19-33.

Antunes and Marco (2012), "Defending against Web Application Vulnerabilities", IEEE Computer Society, Vol:45, No:2, pp;66-72.

Ari Juels, Markus and Tom (2008), “Cache Cookies for Browser Authentication”, IEEE Symposium on Security and Privacy, pp:5-10.

Armando, R.Carbone, L.Compagna, Jorge, Gincarlo and Sorniotti (2012), “An Authentication flaw in browser based single sign on protocols : Impact and remediation’s”, Journal of Computers and Security, Vol:33, pp:41-58.

Aytunc Durlanik, and Ibrahim Sogukpinar (2005), “SIP Authentication Scheme using ECDH”, World Enformatika Society Transactions on Engineering Computing and Technology, Vol;8, pp:350-353.

B.Harris, Hunt (1999), “TCP/IP Security threats and attack methods”, Journal of Computer Communications, Vol:22,No:10, pp:885-897.

Bazara I, Barry and H. Anthony Chan (2007), “A Cross-protocol approach to detect TCP Hijacking attacks”, IEEE International Conference on Signal Processing and Communications, pp:57-60, Dubai, United Arab Emirates.

Ben Adida (2008), “Session Lock : Securing Web Sessions against Eavesdropping”, International Conference on Web Client Security”, pp:517-524, China.

Chomsiri (2007), “HTTPS Hacking Protection”, IEEE 21st International conference on Advanced Information Networking and Applications”,Vol:21, pp:590-597

Chou-Chen Yang, Ren-Chiun Wang, Wei-Ting Liu(2005), “Secure authentication scheme for session initiation protocol”, Computers and Security, Vol:24, No:5, pp:381-386, Elsevier.

Christopher and Jong (2012), “XSSmon: A Perl based IDS for the detection of potential XSS attacks”, IEEE International Conference on Security, pp:1-4,New York

Christopher and Kirda (2009), " Pixy: A Static Analysis Tool for detecting Web Application Vulnerabilities", IEEE Symposium on Privacy and Security, pp:258-263, California.

Collin Jackson and Adam Barth (2008), "Force HTTPS : Protecting High Security Websites from Network Attacks", International Conference on Web Client Security, pp:536-552, China.

Dan Thomsen (1995),"IP spoofing and Session Hijacking", Network Security Journal, Vol:3,No:2, pp:6-11.

Danan Thilakanathan, Shiping Chen, Surya Nepal, Rafael Calvo, Leila Alem (2013), "A platform for secure monitoring and sharing of generic health data in the Cloud", Future Generation Computer Systems,Vol:35, pp:102-113

David Morgan (2006), "Maintaining State in Web Applications", Network Security Journal, Vol:10, No.6, pp:16-18

Evelina Pencheva and Ivaylo Atanasov (2010), "Open Access to call and Session control in Mobile Networks", Cybernetics and Information Technologies, Vol: 10, No:1, pp: 49-63.

F.Wang, Y.Zhang (2007), "A new provably secure Authentication and key agreement mechanisms for SIP using certificate less public key cryptography", International Conference on Computational Intelligence and Security, pp:809-814, China.

Fujan Lai, Dahui Li and Chang Hsieh (2012), "Fighting Identity theft: The coping perspective", Journal of Decision Support Systems, Vol:52, No:2 , pp:353-363

Gary and Su (2008), "Static detection of Cross Site Scripting Vulnerabilities", ACM International Conference on Security and Engineering, pp:171-180, Germany.

Genta and Hiroshi (2009), “An Implementation of the binding mechanism in the web browser for preventing XSS attacks: Introducing the Bind Value Headers”, IEEE International Conference on Availability, Reliability and Security, pp:966-971, Japan

Gill, Smith,Mark and Andrew Clark (2010), “Passive Techniques for detecting the Session Hijack attacks in IEEE 802.11 wireless networks”, Information Security Institute, Queensland University of Technology, Bribane, Australia

Hossain and Mohammad (2011), “S^2XS^2 : A server side approach to automatically detect XSS attacks”, IEEE 9th International conference on Dependable, Automatic and Secure computing, pp:7-14, Sydney

Hsieh, Lo, Lee and Huang (2004), “Implementation of a Proactive Wireless Intrusion Detection System”, In the Proceedings of the 4th IEEE International Conference on Computing and Information Technology, pp: 581-586.

Huyan and Eyas (2011), “Discovering security vulnerabilities and Leaks in ASP.Net websites”, Elsevier Procedia Technology, pp:329-333.

J.cichon, Z.Golebiewski, Miroslae Kutylowski (2012), “ From key pre distribution to key redistribution”, Journal of Theoretical Computer Science, Vol:45, No:3, pp:75-87

Jeffrey Cashion and Mostafa Bassiouni (2011), “Protocol for mitigating the risk of hijacking social networking sites”, IEEE International Conference on Collaborative Computing, Networking Applications and Worksharing , pp:324-331, Florida.

Jorge, Ana, Jose and Benjamin. (2013), “A Taxonomy and survey of attacks on digital signatures”, Journal of Computers and Security, Vol:34, pp:67-112.

Jun zhou, Zhenfu cao, and Xiaolei Dong, Xiaodong lin and Athanasios, Vasilakos (2013), "Securing m-healthcare social networks: Challenges, countermeasures and Future directions", IEEE Wireless Communications for e-health applications", Vol:20, No:4, pp: 12-21.

Jungchae Kim, Byuck jin Lee and Sun K. Yoo (2013), "Design of Real-time Encryption Module for Secure Data Protection of Wearable Healthcare Devices", 35th Annual International Conference of the Engineering in Medicine and Biology Society, pp:2283-2286, Japan.

Kalyani Divi, Mohammed Raza Kanjee and Hong Liu (2010), "Secure Architecture for Healthcare Wireless Sensor Networks", Sixth International Conference on Information Assurance and Security", pp:131-136, Atlanta

Karthikeyan Bhargavan, Ricardo Corin, Cedric Fournet and Andrew D. Gordon (2004), "Secure Sessions for Web Services", ACM Workshop on Secure Web Services, pp:101-106, USA.

Kevin Fu, Emil Sit, Kendra Smith, Nick Feamster (2001), "Dos and Don'ts of Client Authentication on the Web", Proceedings of the 10th USENIX Security Symposium. pp:19-23, Washington.

Khin and Kuan Tan (2011), "Automated removal of Cross Site Scripting vulnerabilities in Web Applications", Journal on Information and Software Technology, Vol:54, No:3, pp:467-478.

Khin Shar and Kuan Tan (2012), "Defending against Cross Site Scripting Attacks", IEEE Computer Society, pp;55-62.

Kuo-Hui Yeh, N.W. Lo, Tzong-Chen Wu, Ta-Chi Yang and Horng-Twu Liaw (2012), "Analysis of an eHealth Care System with Smart Card based Authentication", Seventh Asia Joint Conference on Information Security, pp:59-61, Tokyo

Lanxiang Chen, Dan Feng, Zhan Shi, Feng Zhou(2009), "Using Session Identifiers as Authentication Tokens", IEEE International Conference on Communications, pp:1-5, Germany.

Lee, J.Song, Soohan and won (2011), "Session based classification of internet applications in 3G wireless networks", Journal of Computer Networks, Vol: 55, No: 17, pp: 3915-3931.

Luke Murphey (2004), "Secure Web Based Authentication", IEEE International Conference on Network Security, pp:1-28

Mark Collier (2011), "Analysis of Session Initiation Protocol (SIP) Security", IEEE International Conference on Communications, pp:11-16.

Martin, Bjorn and Joachim (2008), "XSSDS: Server Side detection of Cross Site Scripting attacks", IEEE Annual Computer Security Application Conference, pp;335-344, California

Micheal Howard (2009), "Man-in-the Middle Attack to the HTTPS protocol", IEEE International Conference on Security and Privacy,Vol:7, No:1,pp:78-81, China

Mike and Venkatakrishnan (2009), "BLUEPRINT: Robust Prevention of Cross Site Scripting Attacks for Existing Browsers", 30th IEEE Symposium on Security and Privacy, pp:331-346, Berkeley, CA

Mojib Majidi, Rokhsareh Mobarhan, Amir Hatami Hardoroudi, Abd Samad H-Ismail and Aidin Khodashenas Parchinaki (2011), "Energy Cost Analyses of key Management Techniques for Secure Patient Monitoring in WSN", IEEE Conference on Open Systems, pp:111-115, Malaysia.

Natallia Bielova (2013), "Survey on Java script security policies and their enforcement mechanisms in a web browser", Journal of Logic and Algebraic Programming", Vol:82, No:8, pp: 243-262

Nick, Wannes Meert ,Younan, Johns, Wouter (2009), "SessionShield : Lightweight Protection against Session Hijacking", Proceedings of the Third International Conference on Engineering Secure Software and Systems, pp:87-100, California.

Nikolay Dokev and Ivan Blagoev (2011), "An Approach for automatic transmission of authenticated data over computer networks", Cybernetics and Information Technologies, Vol: 11, No:2, pp:65-82

Nuo Li, Tao Xie, Jin and Liu (2010), "Perturbation based user input validation testing of web applications", Journal of Systems and Software, Vol:83, No:11, pp:2263-2274.

Ori Eisen (2010), "Catching the fraudulent Man-in-the-Middle and Main-in-the – Browser", Network Security, Vol:2010, No:4, pp:11-12

Paul Ritchie (2007), "The security risks of AJAX / Web 2.0 applications", Network Security, Vol:2007, No:3, pp:4-8

Peng, wang, Zhang Wei (2010), "Key technologies of new malicious code developments and defensive measures in communication networks", Journal of China Universities of posts and Telecommunications, Vol:17, No:4, pp:69-73.

Peter Wurzinger and Christian Platzer (2009), “SWAP: Mitigating XSS attacks using a Reverse Proxy”, ICSE Workshop on Software Engineering for Secure Systems, pp:33-39, Vancouver, BC

R.Zhang, X.wang, X.Yang, X.Jiang (2010), “On the billing vulnerabilities of SIP based VOIP systems”, Journal of Computer Networks, Vol:54,No:11,pp:1837-1847.

Rahul and Pankaj (2012), “A survey on web application vulnerabilities Exploitation and Security Engine for SQL Injection”, IEEE International Conference on Communication Systems and Network Technologies”, pp:453-458, Rajkot

Richard Barber (2001), “Hacking Techniques”, Computer Fraud and Security Journal, Vol:3, No:2, pp:9-12.

Roberto Perdisci, Davide Ariu, Prahlad, Giacinto, Wenke Lee (2009), “McPAD: A Multiple classifier system for accurate payload based anomaly detection”, Journal of Computer Networks”, Vol: 53, No: 6 , pp:864-881.

Rongxing Lu, Xiaodong Lin and Xuemin Shen (2013), “SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency”, IEEE Transactions on Parallel and Distributed Systems, Vol: 24, No:3, pp:614-624.

Rui Zhang and Ling Liu, “Security Models and Requirements for Healthcare Application Clouds”, IEEE 3rd International Conference on Cloud Computing, pp:1-8, Miami, Florida

Ryan Farley, X.Wang (2010), “Roving Bugnet : Distributed Surveillance threat and mitigation”, Journal of Computers and Security, Vol:29, No:5, pp:592-602.

San sun, Hawkey and Konstantin (2012), “Systematically breaking and fixing open ID security : Formal Analysis, semi automated empirical evaluation and practical

countermeasures. Elsevier Journal of Computers and Security, Vol:31, No:4, pp:465-483.

Satoshi and Hiji (2006), "A Session Management method to improve web applications usability on Mobile Network", IEEE International Region 10 (TENCON 2006) Conference, pp:1-4. Hong Kong.

Shirley Gaw, Edward W.Felten (2006), "Password Management Strategies for online accounts", International Symposium on Usable Privacy and Security (SOUPS), pp:44-55, Pittsburgh, USA.

Siddharth and Bansal (2012), "Optimized Client Side Solution for Cross Site Scripting", 16th IEEE International Conference on Networks, pp: 1-4, New Delhi.

Suhair Alshehri, Stanisław P. Radziszowski, and Rajendra K. Raj (2012), "Secure Access for Healthcare Data in the Cloud Using Ciphertext-Policy Attribute-Based Encryption", IEEE 28th International Conference on Data Engineering Workshops, pp; 143-146, Arlington, Texas.

T.Chomsiri (2008), "Sniffing Packets on LAN without ARP spoofing", Third IEEE International conference on Convergence and Hybrid Information Technology, pp:472-477, Busan, South Korea

Vinay Kumar (2011), "Three tier verification technique to foil session side jacking attempts", Second Asian International Conference on Internet, pp: 1-4, India

Xiaobo Long and Biplab Sikdar (2010) , "A Mechanism for Detecting the Session Hijack attacks", IEEE Transactions on Wireless Communications, Vol:9, No:4, pp: 1380-1389

Y.Xiang, X.shi, J.Wu, Z.wang, X.Yin (2013), “Sign what you really care about secure BGP AS-Paths efficiently”, Journal of Computer Networks, Vol: 57, No: 10, pp:2250-2265.

Yi-Pin Liao, S.S.Wang (2010), “A new secure password authenticated key agreement scheme for SIP using self certified public keys on elliptic curves”, Journal of Computer Communications”, Vol: 33, No: 3, pp: 372-380.

Yu Sun and Dake (2012), “Model Checking for the Defense against Cross Site Scripting Attacks”, International Conference on Computer Science and Service System, pp:2161-2164, Nanjing, China.

Zhung, Hao and Sun (2010), “An Execution flow based method for detecting Cross Site Scripting Attacks”, 2nd International Conference on Software Engineering and Data Mining, pp:160-165, China.