November 2025: Top 10 Read Articles in International Journal of Security, Privacy and Trust Management (IJSPTM)

International Journal of Security, Privacy and Trust Management (IJSPTM)

http://airccse.org/journal/ijsptm/index.html

ISSN 2277 - 5498 [Online]; 2319 - 4103 [Print]

Contact Us: ijsptm@aircconline.com

DYNAMIC ROOT OF TRUST AND CHALLENGES

Sandeep Romana, Himanshu Pareek and P R Lakshmi Eswari

Center for Development of Advanced Computing,Hyderabad, India

ABSTRACT

Trusted Computing intends to make PC platform trustworthy so that a user can have level of trust when working with it. To build a level of trust TCG gave specification of TPM, as integral part of TCB, for providing root(s) of trust. Further TCG defined Dynamic Root of Trust Measurement in Trusted Computing systems in its specification as a technology for measured platform initialization while system is in running state. The DRTM approach is contrary to Static Root of Trust Measurement where measurements are taken during boot process. In this study, since this technology was first introduced, we list and discuss upon publically available open source solutions that either implement DRTM or are applications of these DRTM based solutions. Further, the challenges faced by the DRTM technology along with observations from authors are listed.

KEYWORDS

SRTM, DRTM, TPM, TCB

For More Details: https://aircconline.com/ijsptm/V5N2/5216ijsptm01.pdf

Volume Link: https://airccse.org/journal/ijsptm/vol5.html

REFERENCES

[1] Latham, Donald C. "Department of Defense trusted computer system evaluation criteria." Department of Defense (1986).

[2] David Challener, Kent Yoder, Ryan Catherman, David Safford, and Leendert Van Doorn. 2007. A Practical Guide to Trusted Computing (First ed.). IBM Press.

[3] Martin, "The ten page introduction to trusted computing," Technical Report RR-08-11, OUCL, December 2008, http://web.comlab.ox.ac.uk/files/1873/RR-08-11.PDF

[4] TCG D-RTM Architecture, Version 1.0.0, June 2013, http://www.trustedcomputinggroup.org/files/static_page_files/5DB17390-1A4B-B294-D029166C91F3512B/TCG_D-RTM_Architecture_v1\%200_Published_06172013.pdf

[5] Trusted Computing Group: TCG Specification Architecture Overview, revision 1.4 (August 2, 2007), http://www.trustedcomputinggroup.org/

[6] Trusted Computing Group, Trusted Platform Module (TPM) Summary, http://www.trustedcomputinggroup.org/resources/trusted platform module tpm summary

[7] Nie, Cong. "Dynamic root of trust in trusted computing." TKK T1105290 Seminar on Network Security. 2007.

[8] Butterworth, John, et al. "Problems with the Static Root of Trust for Measurement."

[9] Intel® Trusted Execution Technology (Intel® TXT), Measured Launched Environment Developer's Guide, May 2014.

[10] Advanced Micro Devices, AMD64 Architecture Programmer's Manual Volume 2: System Programming, Publication no. 24593, Revision 3.23, May 2013.

[11] Bernhard Kauer. 2007. OSLO: improving the security of trusted computing. In Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium (SS'07), Niels Provos (Ed.). USENIX Association, Berkeley, CA, USA, Article 16, 9 pages.

[12] Jonathan M. McCune, Bryan J. Parno, Adrian Perrig, Michael K. Reiter, and Hiroshi Isozaki. 2008. Flicker: an execution infrastructure for tcb minimization. In Proceedings of the 3rd ACM SIGOPS/EuroSys European Conference on Computer Systems 2008 (Eurosys '08). ACM, New York, NY, USA, 315-328. DOI=10.1145/1352592.1352625 http://doi.acm.org/10.1145/1352592.1352625

[13] Brasser, Franz Ferdinand, et al. "Softer Smartcards." Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2012. 329-343.

[14] Justin King-Lacroix and Andrew Martin. 2012. BottleCap: a credential manager for capability systems. In Proceedings of the seventh ACM workshop on Scalable trusted computing (STC '12). ACM, New York, NY, USA, 45-54. DOI=10.1145/2382536.2382545 http://doi.acm.org/10.1145/2382536.2382545

[15] Jonathan M. McCune, Yanlin Li, Ning Qu, Zongwei Zhou, Anupam Datta, Virgil Gligor, and Adrian Perrig. 2010. TrustVisor: Efficient TCB Reduction and Attestation. In Proceedings of the 2010 IEEE Symposium on Security and Privacy (SP '10). IEEE Computer Society, Washington, DC, USA, 143- 158. DOI=10.1109/SP.2010.17 http://dx.doi.org/10.1109/SP.2010.17

[16] Trusted Boot (TBOOT), http://sourceforge.net/projects/tboot/

[17] Joseph Cihula, Trusted Boot: Verifying the Xen Launch, http://wwwarchive.xenproject.org/files/xensummit_fall07/23_JosephCihula.pdf

[18] Flicker: Minimal TCB Code Execution, Mailing Lists, http://sourceforge.net/p/flickertcb/mailman/

[19] Wojtczuk, Rafal, and Joanna Rutkowska. "Attacking Intel trusted execution technology." Black Hat DC (2009).

[20] Wojtczuk, Rafal, Joanna Rutkowska, and Alexander Tereshkin. "Another way to circumvent Intel trusted execution technology." Invisible Things Lab (2009).

[21] Wojtczuk, Rafal, and Joanna Rutkowska. "Attacking Intel TXT via SINIT code execution hijacking." ITL: http://www.invisiblethingslab.com/resources/2011/Attacking_Intel_TXT_ via_SINIT_hijacking.pdf (2011).

AUTHORS

Sandeep Romana obtained his B.Tech from Punjab Technical University and MS in Software Systems from Bits Pilani and is a CISSP. He has more than 8 years of experience in the field of research and development of security software for desktop's and small networks. His areas of research include malware detection and analysis.

Himanshu Pareek received his B.E. degree in 2005 from University of Rajasthan and M.S. By Research degree in 2013 from JNTU, Hyderabad. He has around nine years of

experience in developing and design of end point and gateway based security solutions. His main research interests include malware detection and data science.

MrsP.R.Lakshmi Eswari, is presently working as Joint Director, e-Security R&D, CDAC Hyderabad. She is currently involved in the Research & Development of end system security solutions focusing on anti-Malware & device control solutions. As an outcome of R&D efforts solutions like USB Pratirodh, AppSamvid, Browser JS Guard, Malware Resist etc. are developed by their team.

A WIRELESS FINGERPRINT ATTENDANCE SYSTEM

Mrs. PratimaPatil[1] , Prof. Ajit Khachane[2] and Prof. Vijay Purohit[3]

[1] PG-Student, VIT, Mumbai, India
[2]Dept. of Information Technology, VIT, Mumbai, India
[3]Dept. of EXTC, Mumbai, India

ABSTRACT

In this paper we design a system which takes student attendance and the attendance records are maintained automatically in an academic institute. Taking the attendance manually and maintaining its record till end of year (or even beyond) is very difficult job as well as wastage of time and paper. This necessitates an efficient system that would be fully automatic. Top level design of the system includes marking attendance with the help of a finger-print sensor module and saving the records to a computer or server. Fingerprint sensor module and LCD screen are portable although they can also be fixed to a location for e.g. entry/ exit points. To begin with, a student needs to be registered in the finger-print sensor module. Thereafter every time the student attends a lecture he/ she will place his/her finger on the fingerprint sensor module. The finger-print sensor module will update the attendance record in database. The student can see the notification on LCD screen.

KEYWORDS

Fingerprint module, Fingerprint scanner, Zigbee, LCD etc.

For More Details: https://aircconline.com/ijsptm/V5N4/5416ijsptm02.pdf

Volume Link: http://airccse.org/journal/ijsptm/vol5.html

REFERENCES

[1] LI Jian-po, ZHU Xu-ning, LI Xue, ZHANG Zhi-ming "Wireless Fingerprint Attendance System Based on ZigBee Technology" 2010 IEEE.

[2] MurizahKassim, HasbullahMazlan, NorlizaZaini, Muhammad KhidhirSalleh "Web-based Student Attendance System using RFID Technology" 2012 IEEE.

[3] B. Rasagna, Prof. C. Rajendra "SSCM: A Smart System for College Maintenance" International Journal of Advanced Research in Computer Engineering & Technology, May 2012.

[4] E. Jovanov, D. Raskovic, J. Price, A. Moore, J. Chapman, and A.Krishnamurthy, "Patient Monitoring Using Personal Area Networks of Wireless Intelligent Sensors," Biomedical Science Instrumentation, vol.37, 2001, pp. 373-378.

[5] BarbadekarAshwini, "Performance Analysis of Fingerprint Sensors", Vishwakarma Institute of Technology, Pune, 2010.

[6] Miguel A. Ferrer, Aythami Morales, "Combining hand biometric traits for personal identification", Spain, 2009.

[7] M.A. Meor Said, M.H. Misran, "Biometric attendance", UniversitiTeknikal Malaysia Melaka, Malaysia, 2014.

[8] ShahzadMemon, MojtabaSepasian, WamadevaBalachandran, "Review of Fingerprint Sensing Technologies", Brunel University, West London, United Kingdom, 2008.

[9] Tsai-Cheng Li1, Huan-Wen Wu, "Study of Biometrics Technology Applied in Attendance Management System", Taiwan, 2012.

[10] Mohamed Basheer K P, Raghu C V, "Fingerprint Attendance System for classroom needs", NIT Calicut, Kerala, 2012.

SECURITY SYSTEM WITH FACE RECOGNITION, SMS ALERT AND EMBEDDED NETWORK VIDEO MONITORING TERMINAL

J. Shankar Kartik[1] , K. Ram Kumar[2] and V.S. Srimadhavan[3]

[123]Department of Electronics and Communication Engineering, SRM Easwari Engineering College, Anna University

ABSTRACT

Even though there are various security systems consuming large power are available in market nowadays, robbery rate is very high. We are proposing a novel system to prevent robbery in highly secure areas with lesser power consumption. This system has face-recognition technology which grants access to only authorized people to enter that area. If others enter the place without access using some other means, then the system alerts the security personnel and streams the video captured by the security camera. The face recognition is done using PCA algorithm. The video transmitted is compressed and transmitted by ENVMT. By using this ENVMT, the video can play with lesser bandwidth consumption, latency and jitter.

KEYWORDS

ENVMT, MPEG-4, PCA analysis, ISS, ESS

For More Details: http://airccse.org/journal/ijsptm/papers/2513ijsptm02.pdf

Volume Link: http://airccse.org/journal/ijsptm/vol2.html

REFERENCES

[1] Wang Kechao, Wang Ziangmin, Wang Zhifei, JiaZongfu, Yu Jingwei "Design and implementation of Embedded Network Video Monitoring Terminal" IEEE 2011.

[2] Sutor, S., Matusek, F. , Kruse, F. , Kraus, K. and Reda, R. (2008), 'Large- scale video surveillance system performance parameters and metrics', Internet Monitoring and Protection, ICIMP '08, On Pagc(s) 23 - 30

[3] Bing Li and Jianping Sun (2009) 'Network Video Monitoring Based on Embedded Linux and VC++', International Conference on Advanced Computer Theory and Engineerings.

[4] Dapeng Wu, Yiwei Thomas Hou,Wenwu Zhu, Ya-Qin Zhang, and Jon M. Peha "Streaming video over Internet: Approaches and Directions" IEEE transactions on circuits and systems for video technology, vol. 11, no. 3, March 2001.

[5] Wang Kechao, RenXiangmin, Wang Zhifei, JiaZongfu and Yu Jingwei, (2011) 'Design and implementation of embedded network video monitoring terminal', Computer Science and Automation Engineering (CSAE) ,Volume 3, On Page(s) 211-214.

[6] Yakun Liu and Xiaodong Cheng (2010) 'Design and implementation of embedded Web server based on ARM and Linux', Industrial Mechatronics and Automation (ICIMA) Volume 2, On Page(s) 316- 319.

[7] Yan Liu, RenFaLi, Cheng Xu and Fei Yu (2008) 'Design and Implementation of Embedded Multimedia Surveillance System',Knowledge Discovery and Data Mining Page(s) 570 - 573.

[8] Zhang Songwei and cui ziao (2011) 'Design and implementation of network camera based on TMS320DM365', Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), Page(s) 3864 – 3867.

[9] Marijeta Slavković1, Dubravka Jevtić1 'Face Recognition Using Eigenface Approach' Serbian Journal Of Electrical Engineering Vol. 9, No. 1, February 2012, 121-130.

[10] M. Turk, A. Pentland: Face Recognition using Eigenfaces, Conference on Computer Vision and Pattern Recognition, 3 – 6 June 1991, Maui, HI , USA, pp. 586 – 591.

TRUST-BASED APPROACH IN WIRELESS SENSOR NETWORKS USING AN AGENT TO EACH CLUSTER

Yenumula B. Reddy

Department of Computer science, Grambling State University, Grambling, LA 71245, USA

ABSTRACT

Detection of malicious node in the neighborhood with minimal infrastructure and computations is a requirement. The existing models require more computation, storage, and complex security calculations. These models are inefficient in wireless sensor networks due to their resource limitations. Therefore, an agent-based approach that maintains the node's current status is proposed in this research. In agent-based approach detection is possible through maintaining the ratings of each node. The ratings of a node will be done through the ratio of packet forwarded by packets received. Further, the ratings can be done using the E-commerce models. In E-commerce models, each node votes the successive node depending upon the ratio of packet forwarded by packets received. The update ratings will be done through Sporas formula or Molina's formula or with a combination of both models. Further, the proposed agent-based framework uses reputation of a node through neighbouring nodes as part of trust calculation. The simulations were presented to calculate the trust of a node.

KEYWORDS

Agent-based approach, packet transfer, wireless sensor networks, protocols, trust-based approach, resource

For More Details: https://airccse.org/journal/ijsptm/papers/1112ijsptm02.pdf

Volume Link: https://airccse.org/journal/ijsptm/vol1.html

REFERENCES

[1] Y. B. Reddy and Rastko Selmic., "Secure Packet Transfer in Wireless Sensor Networks – A Trustbased Approach", IARIA- ICN 2011, January 23-28, 2011 - St. Maarten, pp. 218-223.

[2] H. Chen, H. Wu, J. Hu, and C. Gao., "Event-based Trust Framework Model in Wireless Sensor Networks", International Conference on Networking, Architecture, and Storage, 2008, pp. 359-364.

[3] G. Zacharia, A. Moukas, and P. Mae., "Collaborative Reputation Mechanisms for Electronic Marketplaces", Decision Support Systems, Vol. 29, Issue 4, December 2000, pp. 1-7.

[4] S. Ganeriwal, and M. B. Srivastava., "Reputation-based Framework for High Integrity Sensor Networks", Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04), 2004, pp. 66-77.

[5] J. Carbo, J. M. Molina, and J. Davila., "Trust Management through Fuzzy Reputation", International Journal of Cooperative Information Systems", Vol. 12, Issue 1, 2003, pp. 135-155.

[6] J. Carbo, J.M. Molina, and J. Davila., "Comparing Predictions of Sporas vs. a Fuzzy Reputation System", 3rd International Conference on Fuzzy Sets and Fuzzy Systems, 2002 (last accessed on May 24, 2011: www.wseas.us/e-library/conferences/switzerland2002/papers/456.pdf

[7] H. Chen, H. Wu, J. Hu, and C. Gao., "Agent-based Trust Management Model for Wireless Sensor Networks", International Conference on Multimedia and Ubiquitous Engineering, 2008

[8] H. Chen, H. Wu, J. Hu, and C. Gao., "Agent-based Trust Model in Wireless Sensor Networks., "Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing", 2007, pp.119-124.

[9] A. Boukerche, and X. Li., "An Agent-based Trust and Reputation Management Scheme for Wireless Sensor Networks", IEEE GLOBECOMM, 2005.2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04), October 2004, pp 66-77,.

[10] F. G. Momani, and G. M. Perez., "Providing Trust in Wireless Sensor Networks using a Bio-Inspired Technique", NAEC 2008, pp. 1-16.

[11] Mohammad Momani and Subhash Challa (2010). Probabilistic Modelling and Recursive Bayesian Estimation of Trust in Wireless Sensor Networks, Bayesian Network, Ahmed Rebai (Ed.), ISBN: 978-953-307-124-4, InTech, Available from: http://www.intechopen.com/articles/show/title/probabilistic-modelling-and-recursive-bayesianestimation-of-trust-in-wireless-sensor-networks.

[12] E. Aivaloglou, S. Gritzalis, and C. Skianis., "Trust Establishment in ad hoc and Sensor Networks", Lecture notes in computer science, 2006, vol. 4347, pp. 179-194.

[13] E. Kotsovinos, and A. Williams., "BambooTrust: Practical Scalable Trust Management for Global Public Computing", 2006 ACM Symposium on Applied Computing, Dijon, France 2006.

[14] Z. Liang, and W. Shi., "PET: A Personalized Trust Model with Reputation and Risk Evaluation for P2P Resource Sharing", 38 Hawaii Int. conf. on Systems Sciences, 2005, pp. 201-210.

[15] A. Aberer, and Z. Despotovic., "Managing trust in a Peer-2-Peer information system", 10th International Conference on Information and Knowledge management, 2001, pp. 310-317.

[16] M. Momani, and S. Challa., "Survey of Trust Models in different Network Domains", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), Vol.1, No.3, September 2010, pp. 1- 19.

[17] H. Chen., "Task-based Trust Management for Wireless Sensor Networks", International Journal of Security and its applications, vol 3, 2009, 28 Nov.-2 Dec. 2005, pp.1857-1861.

[18] W. Zhang, S. K. Das, and Y. Liu., "A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks", 3rd annual IEEE communications on sensor and ad hoc communications and networks (SECON 06), 2006, pp. 60-69.

[19] W. Zhang, and G. Cao., "Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-based Approach", The 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '05), Miami, USA, 2005.

[20] S. P. Marsh, "Formalising Trust as a Computational Concept", PhD Thesis, University of Stirling, 1994.

[21] A. Josang and R. Ismail., "The Beta Reputation System", 15th Bled Electronic Commerce Conference, 2002, pp. 1-14.

[22] J. Newsome, E. Shi, D. Song and A. Perrig., "The Sybil Attack in Sensor Networks: Analysis & Defenses", Third International Symposium on Information Processing in Sensor Networks, 2004. IPSN 2004. Pp. 259-268, ISBN: 1-58113-846-6.

[23] H. Chan and A. Perrig., "Security and Privacy in Sensor Networks", IEEE Computer Journal, vol. 36, pp. 103-105, 2003.

[24] T. Zia and A. Zomaya., "Security Issues in Wireless Sensor Networks", International conference on Systems and Networks Communication (ICSNC '06), , Tahiti, French Polynesia 2006.

[25] L. Zhou and Z. J. Haas., "Securing Ad-hoc Networks", IEEE Network Magazine, 1999.

[26] B. Przydatek, D. Song and A. Perrig., "SIA: Secure Information Aggregation in Sensor Networks", 1st

International Conference on Embedded Networked Sensor Systems Los Angeles, California, USA 2003.
[27] Y. Wang, G. Attebury and B. Ramamurthy., "A Survey of Security Issues in Wireless Sensor Networks", IEEE Communications Surveys and Tutorials, vol. 8, pp. 2-23, 2006.
[28] F. Stajano and R. Anderson., "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", 8th International Workshop on Security Protocols, Lecture Notes in Computer Science, Springler-Verlag, Berlin, Germany, 1999.
[29] A. Perrig, J. Stankovic and D. Wagner., "Security in Wireless Sensor Networks, Communications of the ACM", vol. 47, pp. 53-57, 2004.
[30] J. P. Walters, Liang, Z. W. Shi and V. Chaudhary., "Wireless Sensor Network Security: A Survey, Security in Distributed, Grid, and Pervasive Computing", Y. Xiao, Ed.: Auerbach Publications, CRC Press, 2006.
[31] D. Zhou., "Security Issues in Ad-hoc Networks", The Handbook of Ad-hoc Wireless Networks Boca Raton, FL, USA: CRC Press, Inc. , 2003, pp. 569 - 582.
[32] P. Papadimitratos and Z. J. Haas., "Securing Mobile Ad-hoc Networks", The Handbook of Adhoc Wireless Networks: CRC Press LLC, 2003.
[33] C. Karlof, N. Sastry, and D. Wagner., "TinySec: A Link Layer Security Architecture for Wireless Sensor Network", Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA, 2004.
[34] S. Zhu, S. Setia and S. Ja., "Sensor Networks", 10th ACM Conference on Computer and Communications Security, Washington D.C., USA, 2003.
[35] C. Karlof and D. Wagner., "ecure Routing in Sensor Networks: Attacks and Countermeasures", First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.
[36] M. Bohge and W. Trappe., "An Authentication Framework for Hierarchical Ad-hoc Sensor Networks", ACM Workshop Wireless security (WiSe '03), San Diego, CA, USA, 2003.
[37] Y. Zhang, W. Liu, W. Lou and Y. Fang., "Location-based Compromise Tolerant Security Mechanisms for Wireless Sensor Networks", IEEE Journal on Selected Areas in Communications, vol. 24, pp. 247-260, 2006.
[38] W. Zhang and G. Cao., "Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-based Approach", 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '05), Miami, USA, 2005
[39] A. Perrig, R. Zewczyk, V. Wen, D. Culler and D. Tygar., "SPINS: Security Protocols for Sensor Networks, Wireless Networks", vol. 8, pp. 521-534, 2002.
[40] F. Ye, H. Luoa, S. Lu and L. Zhang., "Statistical En-route Filtering of Injected False Data in Sensor Networks", Selected Areas in Communications of the ACM, vol. 23, 2005.
[41] H. Baohua, H. Heping and L. Zhengding., "Identifying Local Trust Value with Neural Network in P2P Environment", First IEEE and IFIP International Conference in Central Asia on Internet, Bishkek, Kyrgyz Republic, 2005.
[42] D. Quercia, S. Hailes and L. Capra., "B-trust: Bayesian Trust Framework for Pervasive Computing", Trust 2006 - 4th International Conference on Trust Management, Pisa, Italy, 2006.
[43] F. Azzedin, andM. Maheswaran., "Evolving and Managing Trust in Grid Computing Systems", IEEE Canadian Conference on Electrical and Computer Engineering (CCECE '02), 2002.
[44] B. Dragovic, E. Kotsovinos, S. Hand, and P. R. Pietzuch., "XenoTrust: Event-Based Distributed Trust Management", 14th International Workshop on Database and Expert Systems Applications Prague, Czech Republic, 2003.
[45] B. Shand, N. Dimmock, and J. Bacon., "Trust for Ubiquitous, Transparent Collaboration", Wireless Networks, vol. 10, pp. 711-721, 2003.
[46] V. Cahill, E. Gray, J. M. Seigneur, C. D. Jensen, Y. Chen, B. Shand, N. Dimmock, A. Twigg, J. Bacon, C. W. Wagealla, S. Terzis, P. Nixon, G. D. Marzo Serugendo, C. M. Bryce, K. Carbone, and M. Nielson., "Using Trust for Secure Collaboration in Uncertain Environments", IEEE Pervasive Computing, vol. 2, pp. 52-61, 2003.
[47] P. Michiardi, and R. Molva., "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad-hoc Networks", The IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security Portoroz, Slovenia, 2002.
[48] Y. B. Reddy and Rastko Selmic., "Secure Packet Transfer in Wireless Sensor Networks – A Trustbased Approach", International Journal on Advances in Security, vol 4, no 3&4, 2011.
[49] Y. B. Reddy., "Spectrum selection Through Resource Management in Cognitive Environment", International Journal on Advances in Systems and Measurements, vol 4, no 1&2, year 2011
[50] Y. B. Reddy and Rastko Selmic., Trust-based Packet Transfer in Wireless Sensor Networks, Communications and Information Security (CIS2010), IASTED, Nov 8-10, 2010,USA
[51] Y. B. Reddy, Kafle, S, and Selmic, R., Cooperative and Collaborative Approach for Secure Packet

Transfer in Wireless Sensor Networks, SENSORCOMM 2011, August, 2011.
[52] Y. B. Reddy and Rastko Selmic., No-Regret Learning Approach for Trust-based packet Transfer in Wireless Sensor Networks, SENSORCOMM 2011, August 2011.

Authors

Yenumula B. Reddy, Ph. D. from IIT Delhi, India, Professor of Computer Science, Grambling State University. His research contributions span a number of areas including wireless communications, intrusion detection, data mining, neural networks, intelligent systems, and genetic algorithms. He published more than 100 papers in Journal/Conference proceedings (IEEE/IARIA/IFIP/IASTED) and more than 100 student project presentations in conferences. He is one of the Editor of SENSORCOMM 2011, associate editor of proceedings of ITNG 2009, ITNG 2010, ITNG 2011, and book "Soft Computing Ap plications in Industry. He is editorial board member of Journal BITM Transactions on EECC, Science Academy Transactions on Computer and Communications Networks (SATCCN), and International Journal of Engineering and Industries (IJEI). He is review Committee member of journals IEEE-TVC, IEEE-TVT, and Journal of Communications, and program Committee member of many conferences. He was selected by Louisiana Board for International faculty exchange Program 2010 to conduct "High Performance Computing" course at Pole University, Paris. He was chair of 'International Symposium on Networking and Wireless communications' in connection with ITNG 2008, 2009, 2010, and 2011. He was award winner of best track/Symposium in ITNG 2008-2011. He has successful funding record from the federal and state grants.

A NEW FRAMEWORK FOR SECURING PERSONAL DATA USING THE MULTI-CLOUD

Hassan Saad Alqahtani[1], Paul Sant[1] and Ghita Kouadri-Mostefaoui[2]

[1]IRAC, UCMK, Milton Keynes, UK
[2]Department of Computer Science, UCL, London, UK

ABSTRACT

Relaying On A Single Cloud As A Storage Service Is Not A Proper Solution For A Number Of Reasons; For Instance, The Data Could Be Captured While Uploaded To The Cloud, And The Data Could Be Stolen From The Cloud Using A Stolen Id. In This Paper, We Propose A Solution That Aims At Offering A Secure Data Storage For Mobile Cloud Computing Based On The Multi-Clouds Scheme. The Proposed Solution Will Take The Advantages Of Multi-Clouds, Data Cryptography, And Data Compression To Secure The Distributed Data; By Splitting The Data Into Segments, Encrypting The Segments, Compressing The Segments, Distributing The Segments Via Multi-Clouds While Keeping One Segment On The Mobile Device Memory; Which Will Prevent Extracting The Data If The Distributed Segments Have Been Intercepted.

KEYWORDS

Multi-cloud security, mobile cloud computing, cloud security, secure storage, untrusted environment

For More Details: https://aircconline.com/ijsptm/V4N4/4415ijsptm02.pdf

Volume Link: https://airccse.org/journal/ijsptm/vol4.html

REFERENCES

[1] Kelion, L., 2014. Apple toughens iCloud security after celebrity breach, Available at: http://goo.gl/vyxS3S [Last accessed on October 20, 2015].

[2] Hogan, M., Liu, F., Sokol, A. & Tong, J. 2011, "Nist cloud computing standards roadmap", NIST Special Publication, vol. 35.

[3] Vukolic, M. 2010, "The Byzantine Empire in the Intercloud", SIGACT News, vol. 41, no. 3, pp. 105-111.

[4] AlZain, M.A., Soh, B. & Pardede, E. 2013, "A Byzantine Fault Tolerance Model for a Multi-cloud Computing", Computational Science and Engineering (CSE), 2013 IEEE 16th International Conference on 2013, IEEE, pp. 130-137.

[5] Bessani, A., Correia, M., Quaresma, B., André, F. & Sousa, P. 2013, "DepSky: dependable and secure storage in a cloud-of-clouds", ACM Transactions on Storage (TOS), vol. 9, no. 4, pp. 12.

[6] Verissimo, P., Bessani, A. & Pasin, M. 2012, "The TClouds architecture: Open and resilient cloud-ofclouds computing", Dependable Systems and Networks Workshops (DSN-W), 2012 IEEE/IFIP 42nd International Conference on 2012, IEEE, pp. 1-6.

[7] Spillner, J., Bombach, G., Matthischke, S., Muller, J., Tzschichholz, R. & Schill, A. 2011, "Information Dispersion over Redundant Arrays of Optimal Cloud Storage for Desktop Users", Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on 2011, pp. 1-8.

[8] Resch, J.K. & Plank, J.S. 2011, "AONT-RS: Blending Security and Performance in Dispersed Storage Systems", Proceedings of the 9th USENIX Conference on File and Stroage Technologies USENIX Association, Berkeley, CA, USA, pp. 14.

[9] Storer, M.W., Greenan, K.M., Miller, E.L. & Voruganti, K. 2009, " POTSHARDS—a secure, recoverable, long-term archival storage system ", ACM Transactions on Storage (TOS), 5(2), pp. 5.

[10] Kamara, S., Papamanthou, C. & Roeder, T. "Cs2: A searchable cryptographic cloud storage system".

[11] Tchana, A., Broto, L. & Hagimont, D. 2012, "Approaches to cloud computing fault tolerance", Computer, Information and Telecommunication Systems (CITS), 2012 International Conference on 2012, pp. 1-6.

[12] Zhao, W., Melliar-Smith, P.M. & Moser, L.E. 2010, "Fault Tolerance Middleware for Cloud Computing", Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on 2010, pp. 67-74.

[13] Wu, L., Liu, B. & Lin, W. 2013, "A Dynamic Data Fault-Tolerance Mechanism for Cloud Storage", Emerging Intelligent Data and Web Technologies (EIDWT), 2013 Fourth International Conference on 2013, pp. 95-99.

[14] Rabin, M.O. 1989, "Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance", J.ACM, vol. 36, no. 2, pp. 335-348. [15]

[15] Spillner, J. & Schill, A. 2014, "Towards Dispersed Cloud Computing", Communications and Networking (BlackSeaCom), 2014 IEEE International Black Sea Conference on 2014, pp. 170-174.

[16] Bessani, A., Cutillo, L.A., Ramunno, G., Schirmer, N. & Smiraglia, P. 2013, "The TClouds platform: concept, architecture and instantiations", Proceedings of the 2nd International Workshop on Dependability Issues in Cloud Computing 2013, ACM, pp. 1.

[17] Spillner, J. & Muller, J. 2014, "Tutorial on Distributed Data Storage: From Dispersed Files to Stealth Databases", Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on 2014, pp. 535-536.

[18] Correia, M., Costa, P., Pasin, M., Bessani, A.N., Ramos, F.M. & Verissimo, P. 2012, "On the Feasibility of Byzantine Fault-Tolerant MapReduce in Clouds-of-Clouds.", SRDS 2012, pp. 448-453.

[19] Garraghan, P., Townend, P. & Xu, J. 2011, "Byzantine fault-tolerance in federated cloud computing", Service Oriented System Engineering (SOSE), 2011 IEEE 6th International Symposium on 2011, IEEE, pp. 280-285.

[20] Malik, S. & Huet, F. 2011, "Adaptive Fault Tolerance in Real Time Cloud Computing", Services (SERVICES), 2011 IEEE World Congress on 2011, pp. 280-287.

[21] Abu-Libdeh, H., Princehouse, L. & Weatherspoon, H. 2010, "RACS: a case for cloud storage diversity", Proceedings of the 1st ACM symposium on Cloud computing 2010, ACM, pp. 229-240.

[22] Cachin, C., Haas, R. & Vukolic, M. 2010, Dependable storage in the Intercloud .

[23] Chockler, G., Guerraoui, R., Keidar, I. & Vukolic, M. 2008, Reliable distributed storage.

[24] Stefanov, E., van Dijk, M., Juels, A. & Oprea, A. 2012, "Iris: A scalable cloud file system with efficient integrity checks", Proceedings of the 28th Annual Computer Security Applications Conference 2012, ACM, pp. 229-238.

[25] Wilcox-O'Hearn, Z. & Warner, B. 2008, "Tahoe: the least-authority filesystem", Proceedings of the 4th ACM international workshop on Storage security and survivability 2008, ACM, pp. 21-26.

[26] Popa, R.A., Lorch, J.R., Molnar, D., Wang, H.J. & Zhuang, L. 2011, "Enabling Security in Cloud Storage SLAs with CloudProof.", USENIX Annual Technical Conference.
[27] Basescu, C., Cachin, C., Eyal, I., Haas, R., Sorniotti, A., Vukolic, M. & Zachevsky, I. 2012, "Robust data sharing with key-value stores", Dependable Systems and Networks (DSN), 2012 42nd Annual IEEE/IFIP International Conference on 2012, IEEE, pp. 1-12.
[28] Bowers, K.D., Juels, A. & Oprea, A. 2009, "HAIL: a high-availability and integrity layer for cloud storage", Proceedings of the 16th ACM conference on Computer and communications security 2009, ACM, pp. 187-198.
[29] Ferrer, A. J., Hernández, F., Tordsson, J., Elmroth, E., Ali-Eldin, A., Zsigri, C., et al. 2012, "OPTIMIS: A holistic approach to cloud service provisioning", Future Generation Computer Systems, 28(1), 66-77.
[30] Kecskemeti, G., Kertesz, A., Marosi, A., & Kacsuk, P. 2012, "Interoperable resource management for establishing federated clouds", IGI Global Theory and Practice, Hershey, pp.18-35.
[31] Petcu, D., Crăciun, C., Neagul, M., Panica, S., Di Martino, B., Venticinque, S., et al. 2011, "Architecturing a sky computing platform. Towards a Service-Based Internet", ServiceWave 2010 Workshops, pp. 1-13.
[32] Ismail, I.A., Amin, M. & Diab, H. 2010, "A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps.", IJ Network Security, vol. 11, no. 1, pp. 1-10.
[33] Lian, S., Sun, J. & Wang, Z. 2005, "Security analysis of a chaos-based image encryption algorithm", Physica A: Statistical Mechanics and its Applications, vol. 351, no. 2–4, pp. 645-661.
[34] Ashokkumar, S., Karuppasamy, K., Srinivasan, B. & Balasubramanian V. 2010, "Parallel Key Encryption for CBC and Interleaved CBC," International Journal of Computer Applications, vol. 2, pp. 21-25, 2010.
[35] Harnik, D, Kat, R, Margalit, O, Sotnikov, D, Traeger, A. 2013, "To zip or not to zip: effective resource usage for real-time compression". In: Proceedings of the 11th USENIX conference on file and storage technologies.

AUTHORS

Dr Paul Sant joined the department of Computer Science and Technology (UoB) in September 2005 as a lecturer and he became a Senior Lecturer in September 2006. He was promoted to Principal Lecturer in August 2011. Dr. Paul completed his PhD from King's College, London in 2003 with a thesis entitled "Algorithmics of edge-colouring pairs of 3-regular trees" and prior to this, a BSc. in Computer Science from the University of Liverpool (1999). He is an active member of the British Computer Society and a Chartered Information Technology Professional (CITP) as well as being a fellow of the Higher Education Academy.

Dr Ghita kouadri Mostefaoui is a member of the Advanced Teaching Group, Department of Computer Science, University College London. Ghita has been awarded her PhD in adaptive security, jointly from the University of Fribourg and University Paris VI. Her research interests include cloud computing, automatic extraction of software models and computer science education. Ghita is a fellow of the Higher Education Academy.

Hassan Saad Alqahtani started his PhD March-2014 at university of Bedfordshire. His research interest includes cloud computing, mobile cloud computing, cyber security, and encryption. He received his Master degree from Teesside University in 2012, and his Postgraduate certificate from Essex University in the Telecommunication and Information System.

THE NEW APPROACH TO PROVIDE TRUSTED PLATFORM IN MANET

Renu Dalal[1], Manju Khari[1] and Yudhvir Singh[2]
[1]Department of Computer Science & Engineering, AIACTR, New Delhi, India
[2]Computer Science & Engg. Dept, U.I.E.T M.D University, Rohtak, India

ABSTRACT

In distributed operation, we uses different key management schemes, authentication and many trust models, but in wireless medium having reliability problem, hidden terminal problem etc. To provide authenticated nodes and secured environment is the important issue in MANET. Frequent path breaking, multihop wireless link between mobile nodes, self organization and maintenance are such properties that makes difficult to provide trust in MANET. This paper proposes the new trust scheme, which provides malicious free atmosphere for mobile ad-hoc network. This model first check the authenticity of nodes through challenge response method and then PKI certificate will be given to only authenticated nodes so as to enable the trusted communication platform. At last this paper give the comparisons of ACTP model with other existing trust model.

KEYWORDS

TTP, MANETs, PKI, Symmetric key Cryptography, Trustworthiness, Multihop.

For More Details: https://airccse.org/journal/ijsptm/papers/1612ijsptm01.pdf

Volume Link: https://airccse.org/journal/ijsptm/vol1.html

REFERENCES

[1] C.E. Perkins,' Ad Hoc Networking', 1 st edition. Addision- Wesly Professional, 2001.

[2] Qiuna Niu, "A Trust-Based Message Encryption Scheme for Mobile Ad-Hoc Networks". Second International Workshop on Computer Science and Engineering, 2009.

[3] Wu, B., Wu, J., Fernandez, E., Ilyas, M., and Magliveras, s., 'Secure and Efficient Key Management in Mobile Ad Hoc Wireless Networks'. Journal of Network and Computer Applications (JNCA). Vol. 30, pp. 937-954, 2007

[4] Wong, C., Gouda, M., and Lam, S, 'Secure Group Communications Using Key Graphs'. Proc. of the ACM SIGCOMM'98 conference on Applications, technologies, architectures, and protocols for computer communication, pp 68-79, 1998.

[5] Wallner, D. M., Harder, E. J., and Agee, R. C., 'Key Management for Multicast: Issues and architectures '. Internet Draft, draft-wallner-key-arch-01.txt, 1998.

[6] Renu Dalal, Manju Khari, and Yudhvir Singh, "Survey of Trust Schemes on Ad-hoc Network" CCSIT 2012, Part I, LNICST 84, pp. 170–180, 2012. Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2012

[7] Steiner, M., Tsudik, G., and Waidner, M.,'Cliques: A New approach to Group Key Agreement'. Proc. of the 18 th international Conference on Distributed Computing Systems (ICDCS'98). Pp.380-387, 1998.

[8] Burmester, M. and Desmedt, Y., 'A Secure and Efficient Conference Key Distribution system'. Advances in Cryptology-EUROCRYPT'94, Springer, Berlin. vol. 950. Pp.275-286, 1994.

[9] Kim, Y., Perrig, A., and Tsudik, G., 'Simple and Fault tolerant Key Agreement for Dynamic Collaborative Groups'. Proc. of the 7 th ACM Conference on the Computer and Communications Security, pp. 235-244, 2000.

[10] WEI Chu-yuan, 'A Hybrid Group Key Management Architecture for Heterogeneous MANET', Second International Conferences on Network Security , Wireless Communications and Trusted Computing, 2010.

[11] P. Caballero-Gill and C. Herandez-Goya, "Efficient Public Key Certificate Management for Mobile Ad Hoc Networks," EURASIP journal on wireless Communications and networking, vol. 2011, pp.1-10, 2010.

[12] Behrouz A. Forouzen,"3rd edition Data Communication and Networking", Tata McGraw-Hill Publishing Company Limited, 2004.

MEASURING PRIVACY IN ONLINE SOCIALNETWORKS

Swathi Ananthula, Omar Abuzaghleh, Navya Bharathi Alla, Swetha Prabha Chaganti, Pragna chowdarykaja, Deepthi Mogilineedi

Department Of Computer Science and Engineering, University Of Bridgeport Bridgepo

ABSTRACT

Online Social Networking has gained tremendous popularity amongst the masses. It is usual for the users of Online Social Networks (OSNs) to share information with friends however they lose privacy. Privacy has become an important concern in online social networks. Users are unaware of the privacy risks involved when they share their sensitive information in the network.[1] One of the fundamental challenging issues is measurement of privacy .It is hard for social networking sites and users to make and adjust privacy settings to protect privacy without practical and effective way to quantify , measure and evaluate privacy. In this paper, we discussed Privacy Index (PIDX) which is used to measure a user's privacy exposure in a social network. We have also described and calculated the Privacy Quotient (PQ) i.e. a metric to measure the privacy of the user's profile using the naive approach. [2] The users should be aware of their privacy quotient and should know where they stand in the privacy measuring scale. At last we have proposed a model that will ensure privacy in the unstructured data. It will utilize the Item Response Theory model to measure the privacy leaks in the messages and text that is being posted by the users of the online social networking sites.

KEYWORDS

Online Social Security (OSN), Privacy Measurement, Privacy Index

For More Details: https://airccse.org/journal/ijsptm/papers/4215ijsptm01.pdf

Volume Link: https://airccse.org/journal/ijsptm/vol4.html

REFERENCES

[1] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in Proceedings of the 2005 ACM workshop on Privacy in the electronic society. ACM, 2005, pp. 71–80.

[2] L. Backstrom, C. Dwork, and J. Kleinberg, "Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography," in Proceedings of the 16th international conference on World Wide Web. ACM, 2007, pp. 181–190.

[3] J. DeCew, "Privacy," in The Stanford Encyclopedia of Philosophy, E. N. Zalta, Ed., 2012.

[4] Y. Altshuler, Y. Elovici, N. Aharony, and A. Pentland, "Security and privacy in social networks." Springer, 2013.

[5] M. Huber, M. Mulazzani, E. Weippl, G. Kitzler, and S. Goluch, "Exploiting social networking sites for spam," in Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010, pp. 693–695. [5]

[6] P. Gundecha and H. Liu, "Mining social media: A brief introduction."

[7] B. Fung, K. Wang, R. Chen, and P. S. Yu, "Privacy-preserving data publishing: A survey of recent developments," ACM Computing Surveys (CSUR), vol. 42, no. 4, p. 14, 2010.

[8] R. Agrawal and R. Srikant, "Privacy-preserving data mining," in ACM Sigmod Record, vol. 29, no. 2. ACM, 2000, pp. 439–450.

[9] K. Liu and E. Terzi, "A framework for computing the privacy scores of users in online social networks," in Data Mining, 2009. ICDM'09. Ninth IEEE International Conference on. IEEE, 2009, pp. 288–297.

[10] L. Fang and K. LeFevre, "Privacy wizards for social networking sites," in Proceedings of the 19th international conference on World wide web. ACM, 2010, pp. 351–360.

[11] A. Braunstein, L. Granka, and J. Staddon, "Indirect content privacy surveys: measuring privacy without asking about it," in Proceedings of the Seventh Symposium on Usable Privacy and Security. ACM, 2011, p. 15.

[12] S. Guo and K. Chen, "Mining privacy settings to find optimal privacyutility tradeoffs for social network services," in Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom). IEEE, 2012, pp. 656–665.

[13] J. L. Becker and H. Chen, "Measuring privacy risk in online social networks," Ph.D. dissertation, University of California, Davis, 2009.

[14] J. Anderson, "Privacy engineering for social networks," 2013.

[15] H. R. Lipford, A. Besmer, and J. Watson, "Understanding privacy settings in facebook with an audience view." UPSEC, vol. 8, pp. 1– 8, 2008.

[16] F. Drasgow and C. L. Hulin, "Item response theory," Handbook of industrial and organizational psychology, vol. 1, pp. 577–636, 1990.

[17] H. Mao, X. Shuai, and A. Kapadia, "Loose tweets: an analysis of privacy leaks on twitter," in Proceedings of the 10th annual ACM workshop on Privacy in the electronic society. ACM, 2011, pp. 1–12.

[18] J. Becker, "Measuring Privacy Risk in Online Social Networks," Design, vol. 2, p. 8, 2009.

[19] E. M. Maximilien, T. Grandison, T. Sun, D. Richardson, S. Guo, and K. Liu, "Privacy-as-a-Service : Models , algorithms , and results on the facebook platform," in Web 2.0 Security and privacy workshop, 2009.

[20] K. U. N. Liu, "A Framework for Computing the Privacy Scores of Users in Online Social Networks," Knowl. Discov. Data, vol. 5, no. 1, pp. 1–30, 2010.

[21] N. Talukder, M. Ouzzani, A. K. Elmagarmid, H. Elmeleegy, and M. Yakout, Privometer: Privacy protection in social networks, vol. 1, no. 2. VLDB Endowment, 2010, pp. 141–150.

[22] E. M. Maximilien, T. Grandison, T. Sun, D. Richardson, S. Guo, and K. Liu, "Privacy-as-a-service: Models, algorithms, and results on the facebook platform," in Proceedings of Web, 2009, vol. 2.

[23] C. Akcora, B. Carminati, and E. Ferrari, "Privacy in Social Networks: How Risky is Your Social Graph?," in 2012 IEEE 28th International Conference on Data Engineering, 2012, pp. 9–19.

[24] J. Bonneau and S. Priebusch, "The Privacy Jungle : On the Market for Data Protection in Social Networks," in The Eighth Workshop on the Economics of Information Security, 2009, pp. 1–45.

[25] R. N. Kumar and Y. Wang, "SONET: A SOcialNETwork Model for Privacy Monitoring and Ranking," in The 2nd International Workshop on Network Forensics, Security and Privacy, 2013.

[26] Y. Wang and R. N. Kumar, "Privacy Measurement for Social Network Actor Model," in The 5th ASE/IEEE International Conference on Information Privacy, Security, Risk and Trust, 2013.

[27] M. S. Ackerman, L. F. Cranor, and J. Reagle, “Privacy in ecommerce: examining user scenarios and privacy preferences,” in Proceedings of the 1st ACM conference on Electronic commerce, 1999, vol. 99, no. 1998, pp. 1–8.
[28] A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, “Measurement and analysis of online social networks,” Proc. 7th ACM SIGCOMM Conf. Internet Meas. IMC 07, vol. 40, no. 6, p. 29, 2007.
[29] L. Sweeney, “Uniqueness of simple demographics in the U. S. population,” in Data privacy Lab white paper series LIDAP-WP4, 2000.

DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION PHI FROM FREE TEXT IN MEDICAL RECORDS

Geetha Mahadevaiah[1], Dinesh M.S[1], Rithesh Sreenivasan[1], Sana Moin[1] and Andre Dekker[2]

[1]Philips Research India, Philips Innovation Campus, Manyata Tech Park, Nagavara Bangalore - 560045, India.
[2]Department of Radiation Oncology (MAASTRO), GROW School for Oncology and Developmental Biology, Maastricht University Medical Centre+, Dr Tanslaan 12, 6229ET, Maastricht, The Netherlands

ABSTRACT

Medical health records often contain clinical investigations results and critical information regarding patient health conditions. In these medical records, along with patient health information, patient Protected Health Information (PHI) such as names, locations and date information can co-exist. As per Health Insurance Portability and Accountability Act (HIPAA), before sharing the medical records with researchers and others, all types of PHI information needs to be de-identified. Manual de-identification through human annotators is laborious and error prone, hence, a reliable automated de-identification system is need of the hour.

In this work, various state of the art techniques for de-identification of patient notes in electronic health records were analyzed for their performance, based on the performance quoted in the literature, NeuroNER was selected to de-identify Indian Radiology reports. NeuroNER is a named-entity recognition text de-identification tool developed by Massachusetts Institute of Technology (MIT). This tool is based on the Artificial Neural Networks written in Python and uses Tensorflow machine-learning framework and it comes with five pre-trained models.

To test the NeuroNER models on Indian context data such as name of the person and place, 3300 medical records were simulated. Medical records were simulated by extracting clinical findings, remarks from MIMIC-III data set. For collection of all the relevant Indian data, various websites were scraped to include Indian names, Indian locations (all towns and cities), and Indian Hospital and unit names. During the testing of NeuroNER system, we observed that some of the Indian data such as name, location, etc. were not de-identified satisfactorily. To improve the performance of NeuroNER on Indian context data, along with the existing NeuroNER pre-trained model, a new pre-trained model was added to handle Indian medical reports. Medical dictionary lookup was used to reduce number of misclassifications. Results from all four pre-trained models and the model trained on Indian simulated data were concatenated and final PHI token list was generated to anonymize the medical records to obtain de-identified records. Using this approach, we improved the applicability of the NeuroNER system to Indian data and improved its efficiency and reliability. 2000 simulated reports were used for transfer learning as training set, 1000 reports were used for test set and 300 reports were used for validation (unseen) set

KEYWORDS

De-identification, Free text, Protected Health Information, Medical records, Radiology reports, Indian context data

For More Details: https://aircconline.com/ijsptm/V8N2/8219ijsptm01.pdf

Volume Link: https://airccse.org/journal/ijsptm/vol8.html

REFERENCES

[1] Andrew Arnold, Ramesh Nallapati and William W. Cohen. Exploiting Feature Hierarchy for Transfer Learning in Named Entity Recognition". Proceedings of ACL-08: HLT, 2008

[2] Bin He, Yi Guan, Jianyi Cheng, Keting Cen, and Wenlan Hua. 2015. "Crfs based de-identification of medical records." Journal of biomedical informatics 58:S39–S46.

[3] Bui, D. D. A., M. Wyatt, and J. J. Cimino, "The UAB informatics institute and 2016 CEGS N-GRID de-identification shared task challenge", Journal of Biomedical Informatics, 2017.

[4] Dorr DA, et al: "Assessing the difficulty and time cost of de-identification in clinical narratives". Methods Inf Med 2006, 246-52.

[5] Franck Dernoncourt, Ji Young Lee, Peter Szolovits, Ozlem Uzuner. "De-identification of Patient Notes with Recurrent Neural Networks." arXiv:1606.03475v1 [cs.CL] 10 Jun 2016

[6] Franck Dernoncourt, Ji Young Lee, Peter Szolovits. "NeuroNER: an easy-to-use program for namedentity recognition based on neural networks." arXiv:1705.05487 [cs.CL] 16 May 2017

[7] GPO, U.S: 45 C.F.R. § 46 Protection of Human Subjects 2008 [http://www.access.gpo.gov/nara/cfr/waisidx_08/45cfr46_08.html]

[8] GPO, U.S: 45 C.F.R. § 164 Security and Privacy 2008 [http://www.access.gpo.gov/nara/cfr/waisidx_08/45cfr164_08.html].

[9] Ishna Neamatullah, Margaret M Douglass, Li-wei H Lehman, Andrew Reisner, Mauricio Villarroel, William J Long, Peter Szolovits, George B Moody, Roger G Mark, and Gari D Clifford. "Automated de-identification of free-text medical records." BMC Medical Informatics and Decision Making, 8 (1) (2008), pp. 641-717, 2008 8:32, PMC2526997 2008

[10] Ji Young Lee, Franck Dernoncourt, Peter Szolovits, "Transfer Learning for Named-Entity Recognition with Neural Networks" arXiv:1705.06273 [cs.CL]

[11] Ji Young Lee, Franck Dernoncourt, O¨zlem Uzuner, Peter Szolovits. "Feature Augmented Neural Networks for Patient Note De-identification." arXiv: 1610.09704 [cs.CL] 30 Oct 2016

[12] Kaung Khin, Philipp Burckhardt, Rema Padman, "A Deep Learning Architecture for Deidentification of Patient" Notes: Implementation and Evaluation (arXiv:1810.01570 [cs.CL])

[13] Khalifa, A. and S. Meystre, "Adapting existing natural language processing resources for cardiovascular risk factors identification in clinical notes", Journal of Biomedical Informatics 58 (Supplement), S128-S132, 2015.

[14] Lev Ratinov and Dan Roth. "Design Challenges and Misconceptions in Named Entity Recognition." CoNLL '09 Proceedings of the 13th Conference on Computational Natural Language Learning, Stroudsburg, PA, 2009, pp. 147-155.

[15] Liu, Z., B. Tang, X. Wang, and Q. Chen "De-identification of clinical notes via recurrent neural network and conditional random field" Journal of Biomedical Informatics 75, S34- S42, 2017.

[16] Meystre et al.: "Automatic de-identification of textual documents in the electronic health record: a review of recent research". BMC Medical Research Methodology 2010 10:70

[17] Morrison FP, et al: "Repurposing the clinical record: can an existing natural language processing system de-identify clinical notes?" J Am Med Inform Assoc 2009, 16(1):37-9

[18] Özlem Uzuner, Yuan Luo, Peter Szolovits; "Evaluating the State-of-the-Art in Automatic Deidentification." Journal of the American Medical Informatics Association, Volume 14, Issue 5, 1 September 2007, Pages 550–563

[19] Shweta, Asif Ekbal, Sriparna Saha ,Pushpak Bhattacharyya. "Deep Learning Architecture for Patient Data De-identification in Clinical Records." ClinicalNLP@COLING 2016

[20] Szarvas G, Farkas R, Kocsor A: "A multilingual named entity recognition system using boosting and c4.5 decision tree learning algorithms". 9th Int Conf Disc Sci (DS2006), LNAI 2006, 267-278

[21] Szarvas G, Farkas R, Busa-Fekete R: "State-of-the-art anonymization of medical records using an iterative machine learning framework". J Am Med Inform Assoc 2007, 574-80

[22] Vithya Yogarajan, Michael Mayo, "A survey of automatic de-identification of longitudinal clinical narratives", Bernhard Pfahringer "arXiv:1810.06765 [cs.AI]"

AUTHORS BIOGRAPHY:

Geetha Mahadevaiah, (Corresponding Author) Senior Director at Philips, Research Department, PIC, Bangalore.30+ years of experience in software engineering and management. Areas of interest : Clinical decision support systems, Semantic Web, healthcare applications Bachelor of Engineering in Computer Science and Technology Bangalore University Master of Business Administration, Bangalore University

Dinesh M.S. Senior Principal Scientist at Philips, Research Department, PIC, Bangalore.19+ years of post-doctoral experience in applied research (healthcare domain). Areas of interest: Machine Learning, Pattern recognition and Image Processing Education: Bachelor of Engineering, Master of Technology and Doctor of Philosophy from University of Mysore

André Dekker is a professor of clinical data science at Maastricht University and has been leading the development of prediction models in radiation therapy for many years. He is also coordinator of t he Personal Health Train project, aiming to facilitate citizen science. Areas of interest : Radiomics, Semantic Web, Radiotherapy, machine learning.

DESIGN AND DEVELOPMENT OF A TICKET-BASED SCHEDULING AND LOAD SHARING ALGORITHM FOR OPTIMAL RESOURCE USAGE IN MOBILE COMPUTING ENVIRONMENTS

Natarajan Meghanathan[1] and Sanjeev Baskiyar[2]

[1]Jackson State University, Jackson, MS, USA [2]Auburn University, Auburn, AL, USA

ABSTRACT

Clients in mobile cellular networks lack computing resources to execute complex and data-intensive applications. So the mobile clients purchase tickets from ticket engines installed at stationary servers that are rich in resources. Clients upload computation, resource intensive jobs or applications along with the ticket to the stationary servers. The tickets store the client validity information, deadline before which the stationary servers should execute the job and forward the results to the destination cell, the priority of execution of the job and the run-time history information about the jobs (like the amount resources the job required when it was run before). For simplicity, the stationary servers are assumed to be the base stations. The base stations then schedule the jobs based on the information in the ticket. If the base station at which a job is submitted determines that it will not be able to execute and forward the job to the destination cell before the deadline, the base station forwards it to a supervisory host which can be compared to a base station controller in GSM networks. The supervisory host then schedules the job to any peer base station which can handle the job and forward to the destination before the deadline. The design was simulated using Java. The servers were simulated as shared memory multiprocessor systems. It was determined that on the average there is a 15-60% decrease in turn around time for the jobs executed based on the ticketbased scheduling and load sharing (TB-SLS) model when compared with that of the FIFO or RR models. Also, the percentage deadline guarantee with the ticket model was 30-65% while that of the FIFO and RR models is lower. The simulation was performed on both homogeneous and heterogeneous systems of servers and clients.

KEYWORDS

Ticket, Resource Scheduling, Load Sharing, Mobile Computing, Algorithm Design

For More Details: https://airccse.org/journal/ijsptm/papers/1112ijsptm01.pdf

Volume Link: https://airccse.org/journal/ijsptm/vol1.html

REFERENCES

[1] K. M. Baumgartner and B. W. Wah, "A Global Load Balancing Strategy for a Distributed System," Proceedings of IEEE Workshop on Future Trends in Distributed Computer Systems in the 90's, pp.14-16, 1988.

[2] D. Black, "Scheduling Support for Concurrency and Parallelism in the Mach Operating System," IEEE Computer, v.23, n.5, pp.35-43, 1990.

[3] M. Bozyigit, "History-driven Dynamic Load Sharing for Recurring Applications on Networks of Workstations," Journal of Systems & Software, v.51, no.1, pp. 61-72, 2000.

[4] K. Brown and S. Singh, "Network Architecture for Mobile Computing," Proceedings-IEEE INFOCOM, v.3, pp.1388-1396, 1996.

[5] L. Buttyan and J-P. Hubaux, "Accountable Anonymous Service Usage in Mobile Communication Systems," EPFL SSC Technical Report No. SSC/1999/016, 1999.

[6] V. R. Cheriton, "The V Distributed System," Communications of the ACM, v.13, no.3, pp.314-333, 1988.

[7] A. Croll and E. Packman, "Managing Bandwidth:: Deploying Across Enterprise Networks," Prentice Hall, 2000.

[8] G. Huston, "Internet Performance Survival Guide: QoS Strategies for Multiservice Network," John Wiley & Sons, 2000.

[9] E. Jul and N. Hutchinson, "Grained Mobility in The Emerald System," Transactions on Computer Systems, v.6, no.1, pp.128-133, 1988.

[10] P. D. Le and B. Srinivasan, "A Migration Tool to Support Resource and Load Sharing in Heterogeneous Computing Environments," Computer Communications Journal, pp.361-375, 1997.

[11] P. D. Le, V. Malhotra, N. Mani and B. Srinivasan, "Resource and Load Sharing in Mobile Computing Environments," Proceedings IEEE Region 10th Annual Interantional Conference,v.1, pp.82-85, 1999.

[12] H. C. Lin and C. S. Raghavendra, "A Dynamic Load Sharing Policy with a Central Job Dispatcher," IEEE Transactions on Software Engineering, v.18, no.2, pp.149-158, 1992.

[13] M. Livny and M. Melman, "Load Balancing in Homogeneous Broadcast Distributed Systems," Proceedings of the ACM Computer Network Performance Symposium, v.11, no.1, pp.47-55, 1982.

[14] M. W. Mutka and M. Livny, "Scheduling Remote Processing Capacity in a Workstations-Processor Bank Computer System," Proceedings 7th International IEEE Conference on Distributed Computing Systems, pp. 47-54, 1993.

[15] H. Nishikawa and P. Steenkiste, "A General Architecture for Load Balancing in a DistributedMemory Environment," Proceedings of the 13th IEEE International Conference on Distributed Computing Systems, pp.47-54, 1993.

[16] R. Perlman, "Interconnections: Bridges, Routers, Switches, and Internetworking Protocols," 2nd edition, Addison-Wesley Publishing Co., 1999.

[17] M. Rosing and R. P. Weaver, "Mapping Data to Processors in Distributed Memory Computations," Proceedings of the 5th IEEE Distributed Memory Computing Conference, pp.884-893, 1990.

[18] B. Vickers and B. R. Badrinath, "A Generalizable Service Architecture for Mobile Networks," International Workshop on MoMuc, pp.221-225, 1999.

[19] S. Baskiyar and N. Meghanathan, "Scheduling and Load Sharing in Mobile Computing using Tickets," Proceedings of the ACM-Southeast Conference, pp.175-179, 2001.

POWER AND TRUST BASED SECURED ROUTING APPROACH IN MANET

[1]Arnab Banerjee, [2]Aniruddha Bhattacharyya, [3]Dipayan Bose

Department of Computer Science & Engineering, Institute Of Engineering & Management, Saltlake, India

ABSTRACT

Security in MANET has been one of the most highly rated issues in research field for the last few decades because of its self organizing and cooperative nature, capable of autonomous operation, rapid changing topologies, limited physical security and limited energy resource. So to combat with the security attacks against mobile ad hoc networks we propose a new scheme significantly differing from other existing schemes. In this paper, our proposed scheme, Efficient Secure Routing Protocol in MANET (ESRP) provides a new routing scheme based on trust, an integer value, helping in the selection of administrator inside the network for routing. The comparison between our proposed protocol and other existent secure protocols shows an enhanced and improved performance of our protocol based on the mobile ad hoc parameters. We have also implemented the message confidentiality and integrity in our proposed scheme. Our simulation result shows the robustness, reliability and trustworthiness of our scheme

KEYWORDS

MANET, willingness function, ESRP, trust, administrator

For More Details: https://airccse.org/journal/ijsptm/papers/1213ijsptm04.pdf

Volume Link: https://airccse.org/journal/ijsptm/vol1.html

REFERENCES

[1] Saoucene Mahfoudh, Pascale Minet, "An energy efficient routing based on OLSR in wireless adhoc and sensor networks", 22nd International Conference on Advanced Information Networking and Applications, 2008

[2] Workshops, 2008.T. Clausen, P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", RFC 3626, http://http://tools.ietf.org/html/rfc3626

[3] Fan Hong; Liang Hong; Cai Fu; "Secure OLSR", 19th International Conference on Advanced Information Networking and Applications, 2005. AINA 2005. Page(s): 713 - 718 vol.1

[4] Xiaoqi Li; Lyu, M.R.; Jiangchuan Liu; "A trust model based routing protocol for secure ad hoc networks",Aerospace Conference, 2004. Proceedings. 2004 IEEE,Volume: 2, Page(s): 1286 - 1295

[5] C. Perkins; E. Belding-Royer; S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing." IETF. RFC 3561, July 2003

[6] Songbai Lu, Longxuan Li, Kwok-Yan Lam, Lingyan Jia; "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack",Conference on Computational Intelligence and Security, 2009. CIS '09, Page(s): 421 – 425

[7] Juwad, M.F.; Al-Raweshidy, H.S.; "Experimental Performance Comparisons between SAODV & AODV", Second Asia International Conference on Modeling & Simulation, 2008. AICMS 08, Page(s): 247 - 252

[8] Papadimitratos P., Haas Z. J., Samar P., "The Secure Routing Protocol (SRP) for Ad Hoc Networks", draftsecure-routing-protocol-srp-00.txt, September 2002.

[9] J. Martin Leo Manickam, S.Shanmugavel, "Fuzzy based Trusted Ad hoc On-demand Distance Vector Routing Protocol for MANET", 15th International Conference on Advanced Computing and Communications, 2007

[10] Y.C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Proceedings on Eighth Annual Int'l Conf. Mobile Computing and Networking (MobiCom), 2002, pp. 12-23.

[11] YANG Ya-tao, YUAN Zheng, FANG Yong and ZENG Ping, "A Novel Authentication Scheme Based on Trust-value Updated Model in Adhoc Network", 31st Annual International Computer Software and Applications Conference(COMPSAC 2007), 2007

[12] Raquel Lacuesta Gilaberte, Lourdes Peñalver Herrero, "A secure routing protocol for ad hoc networks based on trust", Third International Conference on Networking and Services (ICNS'07), 2007

[13] Jesus M. Gonzalez, Mohd Anwar, James B.D. Joshi, "Trust-based Approaches to Solve Routing Issues in Ad-hoc Wireless Networks: A Survey", 2011 International Joint Conference of IEEE, TrustCom-11/IEEE CESS-11/FCST-11

[14] Xiang Zeng, Rajive Bagrodia, Mario Gerla,"GloMoSim: A Library for Parallel Simulation of Largescale Wireless Networks", Workshop on Parallel and Distributed Simulation, May 1998

[15] Niigata University, Information & Communication Networks laboratory, "OLSR_Niigata", http://www2.net.ie.niigata-u.ac.jp/olsr-e.php.

[16] Rajive Bagrodia, Richard Meyer, Mineo Takai, Yu-an Chen, Xiang Zeng, Jay Martin, Ha Yoon, "Parsec: A Parallel Simulation Environment for Complex Systems", October 1998

[17] Dipayan Bose, Arnab Banerjee, Aniruddha Bhattacharyya, Himadri Nath Saha and Debika Bhattacharyya, et al.: An Efficient Approach to Secure Routing in MANET, Advances in Intelligent Systems and Computing, 1, Volume 176, Advances in Computing and Information Technology, Pages 765-776, DOI: 10.1007/978-3-642-31513-8_78

AUTHORS

ARNAB BANERJEE Having completed B.Tech in Computer Science & Engineering from AIEM, Durgapur, he pursued M.Tech degree in Computer Science & Engineering Department from Institute Of Engineering an d Management, Saltlake.While pursuing M.Tech, he have gathered a year experience in teaching in Institute Of Engineering and Management as Lecturer Trainee in the Computer Science & Engineering Department. His interest includes Algorithm, AI, Fuzzy Logic, Automata.

ANIRUDDHA BHATTACHARYYA He did his B.Tech in Electronics & Instrumentation from Academy of Technology, Hooghly and his M.Tech in Computer Science & Engineering from Institute of Engineering & Management, Saltlake, Kolkata. He has worked in software development industry for more than 2 year s. His interest includes software development, HPC/Parallel/GPU Computing, embedded system design & AI.

DIPAYAN BOSE Having completed B.Tech in Computer Science & Engineering from A IEM, Durgapur, he pursuaded M.Tech degree in Computer Science & Engineering Department from Institute Of Engineering and Management, Saltlake. Has interest in networking operating system(LINUX) and Algorithm.