September 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

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.

A TRUST MANAGEMENT FRAMEWORK FOR VEHICULAR AD HOC NETWORKS

RezviShahariar and Chris Phillips

School of Electronic Engineering and Computer Science, Queen Mary, University of London, London, UK

ABSTRACT

Vehicular Ad Hoc Networks (VANETs) enable road users and public infrastructure to share information that improves the operation of roads and driver experience. However, these are vulnerable to poorly behaved authorized users. Trust management is used to address attacks from authorized users in accordance with their trust score. By removing the dissemination of trust metrics in the validation process, communication overhead and response time are lowered. In this paper, we propose a new Tamper-Proof Device (TPD) based trust management framework for controlling trust at the sender side vehicle that regulates driver behaviour. Moreover, the dissemination of feedback is only required when there is conflicting information in the VANET. If a conflict arises, the Road-Side Unit (RSU) decides, using the weighted voting system, whether the originator is to be believed, or not. The framework is evaluated against a centralized reputation approach and the results demonstrate that it outperforms the latter.

KEYWORDS

VANET, Trust Management, Security, Tamper Proof Device, Malicious Behaviour

For More Details: https://aircconline.com/ijsptm/V12N1/12123ijsptm02.pdf

Volume Link: https://airccse.org/journal/ijsptm/vol12.html

REFERENCES

[1] Shrikant Tangade, Sunilkumar S. Manvi, "Trust management scheme in VANET: Neighbour communication-based approach," in Proc. IEEE Int. Conf. on Smart Technol. for Smart Nat. (SmartTechCon)., Bengaluru, India, 2017, pp. 741-744.

[2] Zhexiong Wei, Fei Richard Yu, Azzedine Boukerche, "Trust based security enhancements for vehicular ad hoc networks," in Proc. of the 4th ACM Int. Symp. on Dev. and Anal. of Intell. Veh. Netw. and Appl. (DIVANet)., Montreal, Canada, 2014, pp. 103-109.

[3] Shrikant Tangade, Sunilkumar S. Manvi, "CBTM: Cryptography based trust management scheme for secure vehicular communications," in Proc. IEEE 15th Int. Conf. on Control., Autom., Robot. and Vis. (ICARCV)., Singapore, 2018, pp. 325-330.

[4] Dahiya, Rohan, Frank Jiang, Robin Ram Doss, "A Feedback-Driven Lightweight Reputation Scheme for IoV," in Proc. IEEE 19th Int. Conf. on Trust. Secur. and Priv. in Comput. and Commun. (TrustCom)., Guangzhou, China, 2020, pp. 1060-1068.

[5] Farhan Ahmad, Virginia NL Franqueira, Asma Adnane, "TEAM: A trust evaluation and management

[6] framework in context-enabled vehicular ad-hoc networks," IEEE Access, vol. 6, pp. 28643-28660, May. 2018.

[7] Tahani Gazdar, Abdelfettah Belghith, Hassan Abutair, "An enhanced distributed trust computing protocol for VANETs," IEEE Access, vol. 6, pp. 380-392, Oct. 2017.

[8] Nadia Haddadou, Abderrezak Rachedi, Yacine Ghamri-Doudane, "A job market signaling scheme for incentive and trust management in vehicular ad hoc networks," IEEE trans. on Veh. Technol., vol. 64, no. 8, pp.3657-3674. Sept. 2014.

[9] Ricardo Mühlbauer, João Henrique Kleinschmidt, "Bring your own reputation: A feasible trust system for vehicular ad hoc networks," J. of Sens. and Actuator Netw., vol. 7, no. 3, p.37, Sept. 2018.

[10] Siri Guleng, Celimuge Wu, Xianfu Chen, Xiaoyan Wang, Tsotumu Yoshinaga, Yusheng Ji,"Decentralized Trust Evaluation in Vehicular Internet of Things," IEEE Access, vol. 7, pp. 15980-15988, Jan. 2019.

[11] Zhaojun Lu, Gang Qu, Zhenglin Liu, "A survey on recent advances in vehicular network security,trust, and privacy," IEEE Trans. on Intell. Transp. Syst., vol. 20, no. 2, pp.760-776, Apr. 2018.

[12] Yu-Chih Wei, Yi-Ming Chen, "Adaptive decision making for improving trust establishment in vanet," in Proc IEEE 16th Asia-Pacific Netw. Oper. and Manag. Symp. (APNOMS)., Hsinchu, Taiwan, 2014, pp. 1-4.

[13] Wenjia Li, Houbing Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," IEEE Trans. on Intell. Transp. Syst., vol. 17, no. 4, pp. 960-969, Nov. 2015.

[14] Zhe Yang, Kan Yang, Lei Lei, Kan Zheng, Victor C.M. Leung, "Blockchain-based decentralized trust management in vehicular networks," IEEE Internet of Things J., vol. 6, no. 2, pp.1495-1505, May. 2018.

[15] Seyed Ahmad Soleymani, Abdul Hanan Abdullah, Mahdi Zareei, Mohammad Hossein Anisi, Cesar Vargas-Rosales, Muhammad Khurram Khan, ShidrokhGoudarzi , "A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing," IEEE Access, vol. 5, pp. 15619- 15629, Jul. 2017.

[16] Qin Li, Amizah Malip, Keith M. Martin, Siaw-Lynn Ng, Jie Zhang,, "A reputation-based

announcement scheme for VANETs," IEEE Trans. on Veh. Technol., vol. 61 no. 9, pp.4095-4108, Nov. 2012.

[17] Sarah Ali Siddiqui, Adnan Mahmood, Quan Z. Sheng, Hajime Suzuki, Wei Ni, "A time-aware trust management heuristic for the Internet of Vehicles," In 2021 IEEE 20th Int. Conf. on Trust., Secur. and Priv. in Comput. and Commun. (TrustCom)., Shenyang, China, Oct. 2021. pp. 1-8,

[18] Muhammad Usman Aftab, Mehdi Hussain, Anders Lindgren, Abdul Ghafoor, "Towards a distributed ledger based verifiable trusted protocol for VANET", in 2021 Int. Conf. on Digit. Future and Transp. Technol. (ICoDT2),. Islamabad, Pakistan, May. 2021, pp. 1-6 .

[19] Chaker Abdelaziz Kerrache, Nasreddine Lagraa, Carlos T. Calafate, Abderrahmane Lakas, "TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs," Veh. Commun., vol. 9, pp. 254-267, Dec. 2017.

[20] Sashi Gurung, Dan Lin, Anna Squicciarini , Elisa Bertino , "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks," in Proc. Netw. and Syst. Secur. (NSS)., Berlin Heidelberg, Germany, Springer, 2013, pp. 94-108.

[21] Danda B. Rawat, Gongjun Yan, Bhed B. Bista, Michele C. Weigle, "Trust on the Security of Wireless Vehicular Ad-hoc Networking," Ad Hoc Sens. Wirel. Netw., vol. 24, no. 3/4, pp. 283-305, Jan. 2015.

[22] Guanghao Wang, Yue Wu, "BIBRM: A bayesian inference-based road message trust model in vehicular ad hoc networks," in Proc 13th Int. Conf. on Trust. Secur. and Priv. in Comput. and Commun. (TrustCom)., Beijing, China, 2014, pp. 481-486.

[23] Karim Rostamzadeh, Hasen Nicanfar, Narjes Torabi, Sathish Gopalakrishnan, Victor C. M. Leung, "A context-aware trust-based information dissemination framework for vehicular networks," IEEE Internet of Things J., vol. 2, no. 2, pp.121-132, Apr. 2015.

[24] Ibrahim Abdo Rai, Riaz Ahmed Shaikh, Syed Raheel Hassan, "A hybrid dual-mode trust management scheme for vehicular networks," Int. J. of Distrib. Sens. Netw., vol. 16 no. 7, pp.1550147720939372, Jul. 2020.

[25] Yao Xuanxia, Zhang Xinlei, Ning Huansheng, Li Pengjian, "Using trust model to ensure reliable data acquisition in VANETs," Ad Hoc Netw., vol. 55, pp.107-118, Feb. 2017.

[26] Rasha Jamal Atwa, Paola Flocchini, Amiya Nayak, "Risk-based trust evaluation model for VANETs," In 2020 Int. Symp. on Netw., Comput. And Commun. (ISNCC)., Montreal, QC, Canada, Oct. 2020, pp. 1-6.

[27] Honghao Gao, Can Liu, Yuyu Yin, Yueshen Xu, Yu Li, "A hybrid approach to trust node assessment and management for vanets cooperative data communication: Historical interaction perspective," IEEE Trans. on Intell. Transp. Sys. pp . vol. 23, no. 9, pp. 1-10, Nov. 2021.

[28] Zhigang Yang, Ruyan Wang, Dapeng Wu, Boran Yang, Puning Zhang, "Blockchain-enabled Trust Management Model for the Internet of Vehicles," IEEE Internet of Things J., Oct. 2021.

[29] Xiao Chen, Jie Ding, Zhenyu Lu, "A decentralized trust management system for intelligent transportation environments," IEEE Trans. on Int. Transp. Sys., vol. 23, no. 1, pp.558-571, Jan. 2022.

[30] Car2x, Vehicles in Network Simulation (Veins) v5.0 (Version 5.0), car2x, September 19, 2022. https://veins.car2x.org/download/.

[31] OpenSim Limited, Objective Modular Network Testbed in C++ (OMNeT++) v5.5.1 (Version 5.5.1), omnetpp.org, September 19, 2022. https://omnetpp.org/software/2019/05/31/omnet-5-5-released.

[32] The German Aerospace Center, Simulation of Urban Mobility (SUMO) v1.2.0. (Version 1.2.0), sourceforge, September 19, 2022. https://sourceforge.net/projects/sumo/files/sumo/version%201.2.0/.

AUTHORS

RezviShahariar received his B.Sc. degree in Computer Science from the University of Dhaka, Bangladesh in 2006; and an M.S. degree in Computer Science in 2007 from the same institution. After some time as a lecturer at the University of Asia Pacific, Dhaka, Bangladesh, he is now an Assistant Professor at the Institute of Information Technology, University of Dhaka, whilst pursuing a PhD at Queen Mary University of London. His research interests include wireless network analysis with an emphasis on trust, security in VANETs, and the application of machine learning to security.

Chris Phillips (MIEEE) received a BEng. Degree in Telecoms Engineering from Queen Mary, University of London (QMUL) in 1987 followed by a PhD on concurrent discrete event-driven simulation, also from QMUL. He then worked in industry as a hardware and systems engineer with Bell Northern Research, Siemens Roke Manor Research and Nortel Networks, focusing on broadband network protocols, resource management and resilience. In 2000 he returned to QMUL as a Reader. His research focuses on management mechanisms to enable limited resources to be used effectively in uncertain environments.

MANAGING THE INFORMATION SECURITY ISSUES OF ELECTRONIC MEDICAL RECORDS

NisreenInnab

Faculty of Computer and Information Security, Naif Arab University for Security Sciences, Al-Riyadh, Saudi Arabia

ABSTRACT

All healthcare providers should have enough knowledge and sufficient information to understand the potential risk, which can lead to a breach in the Jordanian health information system (Hakeem program). This study aims to emphasise the importance of sharing sensitive health information among healthcare providers, create laws and regulations to keep the electronic medical records secure, and increase the awareness about health information security among healthcare providers. The study conducted seven interviews with medical staff and an information technology technician. The study results showed that sharing sensitive information in a secure environment, creating laws and regulations, and increasing the awareness about health information security render the electronic medical records of patients more secure and safe.

KEYWORDS

Electronic Medical Records Security, Health Records, Data Breach, Hakeem Program.

For More Details: https://aircconline.com/ijsptm/V7N4/7418ijsptm02.pdf

Volume Link:http://airccse.org/journal/ijsptm/vol7.html

REFERENCES

[1] Key, D. &Ferneini, E., (2015) "Focusing on Patient Safety: the Challenge of Securely SharingElectronic Medical Records in Complex Care Continuums", ConnecticutMedicine, Vol. 79, No. 8, pp 481- 485.

[2] Miller, A & Tucker, (2009) "Privacy protection and technology diffusion: the case of electronic medical records", Management Science, Vol. 55, No. 7. pp 1077–1093.

[3] Kazley, A. &Ozcan, Y., (2007) "Organizational and environmental determinants of hospital EMR adoption: A national study", J. Medical Systems, Vol. 31, No. 5, pp 375–384.

[4] Marvin (2017) "Health Information Technology: Integration, Patient Empowerment, and Security",Am J Health-Syst Pharm, Vol. 74 No. 2, Pp 36-38.

[5] Humaidi, N. &Balakrishnan, V., (2015) "The moderating effect of working experience on health information system security policies compliance behavior", Malaysian Journal of Computer Science, Vol.28, No. 2, pp 70-92.

[6] Khan, S. &Hoque, S., (2016) "Digital health data: a comprehensive review of privacy and security risks and some recommendations", Computer Science Journal of Moldova, Vol. 24, No. 2, pp 273- 292.6

[7] Dua', A., Marini, O &Hasniza, Y., (2013) "Implementation of an EHR system (Hakeem) in Jordan: challenges and recommendations for governance", HIM-Interchange, Vol. 3, No. 3, pp 10-12.

[8] Electronic Health Solutions, (2017) "Benefits of Hakeem Program", Retrieved from http://ehs.com.jo/hakeem-program/benefits-hakeem

[9] Howard, P.,(2014) "Data Breaches in Europe: An Analysis of Reported Breaches of Compromised Personal Records in Europe", Center for Media, Data and Society Central European University. Retrieved from: http://cmds.ceu.edu/sites/cmcs.ceu.hu/files/attachment/article/663/databreachesineurope.pdf

[10] Ponemon Institute, (2015 "Cost of data breach study: Global analysis", Ponemon Institute, Research Report.

[11] Ponemon Institute, (2015) "Fifth annual benchmark study on privacy & security of healthcare data", Ponemon Institute, Research Report.

[12] Khan, S. &Hoque, A., (2015) "Development of nationalhealth data warehouse for data mining", Database Systems Journal, Vol. 6, No. 1, pp 3–13.

[13] Orel, A. & Bernik, I., (2013) "Implementing healthcare information security: standards can help", Implementing Healthcare Information Security: Standards Can Help, Vol. 186, pp 195-199.

[14] Luethi, M. & Knolmayer, G., (2009) "Security in health information systems: Anexploratory comparison of U.S. and Swiss hospitals", Hawaii International Conference on System Sciences.

[15] Vest, J. & Kash, B., (2016) "Differing strategies to meet information-sharing needs: Publicly supported community health information exchanges versus health systems' enterprise health information exchanges", The Milbank Quarterly, Vol. 94, No. 1, pp 77-108.

[16] Bansal, G., Zahedi, F., &Gefen, D., (2010) "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online", Decision Support Systems, Vol 49, No 2, pp 138-150.

[17] Tipton, H. & Krause, M. (2015) Information Security Management Handbook, 6thed. Northwestern:

CRC Press.

[18] Aydın O. &Chouseinoglou, O., (2013). "Fuzzy assessment of health information system users' security awareness", Journal of Medical Systems, Vol. 37, No. 6, pp 84-99.

AUTHOR

Dr. NisreenInnab got her Ph.D. in 2008 in Computer Information System, she was employed as full time lecturer, Assistant Professor and MIS department Chairperson at University of Business and Technology in Saudi Arabia, Jeddah from 2007 to 2010. Then she was worked from May 2011 to August 2014 as a honorary researcher and master thesis examiner in the school of science and technology at University of New England, Armidale, Australia. Finally, from September / 2016 till now she works in the department of information security at Naif Arab University for Security Sciences, Riyadh, Saudi Arabia.
She published nine papers in international journals and conferences. Her current research interests are: information security, data mining, machine learning, modeling and simulation, ontology, modeling diagrams.

TRUST: DIFFERENT VIEWS, ONE GOAL

Mubarak Almutairi

College of Computer Science & Engineering, University of HafrAlbatin, HafrAlbatin, Saudi Arabia

ABSTRACT

A thorough review of trust models is carried out in this paper to reveal the key capabilities of existing trust models and compare how they differ among disciplines. Trust decisions are risky due to uncertainties and the loss of control. On the other hand, not trusting might mean giving up some potential benefits. Advances in electronic transactions, mutliagent systems, and decision support systems create a necessity to develop trust and reputation models. The development of such models will allow for trust reasoning and decisions to be made in situations with high risk and uncertainty. In recent years, several attempts have been made to model reputation and trust. However, perceiving trust differently and the lack of having a unified trust definition are among the main causes of the proliferation of many trust models across different disciplines.

For More Details: https://aircconline.com/ijsptm/V6N1/6117ijsptm01.pdf

Volume Link: https://airccse.org/journal/ijsptm/vol6.html

REFERENCES

[1] Abdul-Rahman, A., and Hailes, S., "Supporting trust in virtual communities", Proceedings of the Hawaii International Conference on System Sciences, Maui, Hawaii, 2000.

[2] AL-Mutairi, M., Hipel, K., and Kamel, M., "Modeling Trust Using a Fuzzy Logic Approach", Proceedings of International Symposium on Systems and Human Science, USA: San Francisco, 2005.

[3] Amazon. Amazon Auctions. http://auctions.amazon.com, 2002.

[4] Ashri, R., Ramchurn, S., Sabater, J., Luck, M., and Jennings, N., "Trust evaluation through relationship analysis", Proceedings of the 4th International Joint Conference on autonomous Agents and Multi-Agent Systems, 2005, pp. 1005–1012.

[5] Bacharach, M., and Gambetta, D., "Trust in Society", in K. Cook (Ed.), Trust in signs. New York:Russell Sage Foundation, 2001.

[6] Baier, A., "Trust and Antitrust", Ethics 96, 1986, pp. 231-260.

[7] Barber, K., and Kim, J., "Belief Revision Process based on Trust: Simulation Experiment", Proceedings of the Fourth Workshop on Deception, Fraud and Trust in Agent Societies, Montreal, Canada, 2001, pp. 1–12.

[8] Bhattacherjee, A., "Individual trust in online firms: scale development and initial trust", Journal of Management Information Systems, 2002, 19(1), 213–243.

[9] Bromley, D., "Reputation, Image and Impression Management", John Wiley & Sons, 1993.

[10] Beth, T., Borcherding, M., and Klein, B. "Valuation of trust in open networks", Proceedings of the 3rd European Symposium on Research in Computer Security, 1994, pp 3–18.

[11] Blaze, M., Feigenbaum, J., Ioannidis, J., and Keromytis, A. "The role of trust management in distributed system security", Lecture Notes in Computer Science, 1999, vol. 1603: pp. 185–210.

[12] Blaze, M., Feigenbaum, J., and Lacy, J., "Decentralized trust management", Proceedings of IEEE Symposium on Security and Privacy, 1996, pp. 164–173.

[13] Brainov, S., and Sandholm, T., "Contracting with uncertain level of trust", Proceedings of the 1st ACM conference on Electronic commerce, New York, NY, USA. ACM Press, 1999, pp. 15–21.

[14] Brin, S., and Page, L., "The anatomy of a large-scale hypertextual Web search engine", Computer Networks and ISDN Systems, 1998, vol. 30(1–7), pp. 107–117.

[15] Bromley, D., Reputation, Image and Impression Management. New York: John Wiley & Sons.

[16] Buchegger, S., and Boudec, J.-Y. Le, "A Robust Reputation System for Mobile Ad-hoc Networks", Technical Report IC/2003/50, EPFL-IC-LCA, 2003a.

[17] Buchegger, S., and Boudec, J.-Y. Le, "The Effect of Rumor Spreading in Reputation Systems for Mobile Ad-hoc Networks", Proceedings of the Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, 2003b.

[18] Buskens, V., "The social structure of trust", Social Networks, 1998, vol. 20, pp. 265–289.

[19] Cahill, V., and Shand, B., Gray, E. et al., "Using trust for secure collaboration in uncertain environments", Pervasive Computing, 2003, vol. 2(3), pp. 52– 61.

[20] Carbo, J., Molina, J., and Davila, J., "Comparing Predictions of SPORAS vs. a Fuzzy Reputation Agent System", Third International Conference on Fuzzy Sets and Fuzzy Systems, Interlaken, 2002, pp. 147–153.

[21] Carbone, M., Nielsen, M., and Sassone, V., "A formal model for trust in dynamic networks", Proceedings of International Conference on Software Engineering and Formal Methods (SEFM'03), Brisbane, 2003.

[22] Carter, J., Bitting, E., and Ghorbani, A., "Reputation Formalization for an Information-Sharing MultiAgent System", Computational Intelligence, 2002, vol. 18(2), pp. 515–534.

[23] Castelfranchi, C., and Falcone, R., "Principles of Trust for MAS: Cognitive Anatomy, Social Importance, and Quantification," Proceedings of the International Conference on Multi-Agent Systems (ICMAS'98), Paris, France, 1998, pp. 72–79.

[24] Castelfranchi, C., Falcone, R., and Pezzulo, G., "Trust in information sources as a source for trust: a fuzzy approach", Proceedings of the second international joint conference on Autonomous agents and multiagent systems, New York, NY, USA. ACM Press, 2003, pp. 89–96.

[25] Celentani, M., Fudenberg, D., Levine, D., and Psendorfer, W., "Maintaining a Reputation Against a Long-Lived Opponent", Econometrica, 1966, vol. 64(3), pp. 691–704.

[26] Chang, R., "Credible Monetary Policy with Long-Lived Agents: Recursive Approaches", Journal of Economic Theory, 1998, vol. 81, pp. 431-461.

[27] Chari, V., and Kehoe, P., "Sustainable Plans", Journal of Political Economy, 1990, vol. 98, pp. 783–802.

[28] Chen, M., and Singh, J., "Computing and using reputations for internet ratings", Proceedings of the Third ACM Conference on Electronic Commerce (EC'01), ACM, 2001.

[29] Chirita, P., Nejdl, W., Schlosser, M., and Scurtu, O., "Personalized reputation management in p2p networks", Proceedings of the Trust, Security and Reputation Workshop held at the 3rd International Semantic Web Conference, 2004.

[30] Conte, R., and Paolucci, M., Reputation in Artificial Societies: Social Beliefs for Social Order. Kluwer Academic Publishers, 2002.

[31] Corritore, C., Wiedenbeck, S., and Kracher, B., "The elements of online trust", CHI '01: CHI '01 extended abstracts on Human factors in computing systems, New York, NY, USA. ACM Press, 2001, pp. 504–505.

[32] Cvetkovivh, G. and Lofstedt, R., Social Trust and the Management of Risk. Earthscan Publications,1999.

[33] Damiani, E. et al., "A reputation-based approach for choosing reliable resources in peer-to-peer networks", Proceedings of the 9th ACM conference on Computer and Communications Security (CCS'02), ACM, 2002, pp. 207–216.

[34] Dellarocas, C., "The digitalization of Word-Of-Mouth: Promise and Challenges of Online Reputation Mechanisms", Management Science, 2003, 49(10).

[35] Dellarocas, C., "Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior", ACM Conference on Electronic Commerce, 2000, pp. 150–157.

[36] Demolombe, R., "To Trust Information Sources: a Proposal for a Modal Logic Framework. Trust

and Deception in Virtual Societies," in C. Castelfranchi, and Yao-Hua Tan (Eds.), Trust and Deception in Virtual Societies. Kluwer Academic Publisher, 2001.

[37] Deutsch, M., The Resolution of Conflict. New Haven: Yale University Press, 1973.

[38] Ding, L., Kolari, P., Ganjugunte, S., Finin, T., and Joshi, A., "Modeling and evaluating trust network inference", Proceedings of the 7th International Workshop on Trust in Agent Societies at AAMAS, 2004.

[39] Doney, M., and Cannon, J., "An examination of the nature of trust in buyer–seller relationships", Journal of Marketing, 1997, vol. 61: pp. 35–51.

[40] eBay. http://www.eBay.com, 2002.

[41] Einwiller, S., Geissler, U., and Will, M., "Engendering Trust in Internet Businesses Using Elements of Corporate Branding", Proceedings of the 2000 Americas Conference on Information Systems (AMCIS), USA: Long Beach, 2000.

[42] Einwiller, S., and Will, M., "The Role of Reputation to Engender Trust in Electronic Markets", Proceedings of the fifth International Conference on Corporate Reputation, Identity, and Competitiveness, France: Paris, 2001.

[43] Esfandiari, B., and Chandrasekharan, S., "On How Agents Make friends: Mechanisms for Trust Acquisition", Proceedings of the fourth Workshop on Deception, Fraud and Trust in Agent Societies, Montreal, Canada, 2001, pp. 27–34.

[44] Falcone, R., and Castelfranchi, C., Social Trust: A Cognitive Approach. Kluwer Academic Publisher, 2001.

[45] Ferrary, M., "Trust and social capital in the regulation of lending activities", Journal of SocioEconomics, 2002, vol. 235: pp. 1–27.

[46] Friedman, B., Peter H. Khan, J., and Howe, D., "Trust online", Communication of ACM, 2000, vol.43(12): pp. 34–40.

[47] Friedman, M., A Program for Monetary Stability. Fordham University Press, New York, 1960.

[48] Gambetta, D., "Can we trust trust?", in: D. Gambetta (Ed.), Trust: Making and Breaking Cooperative Relations, Basil Blackwell, Oxford, 2000.

[49] Ganesan, S., "Determinants of long-term orientation in buyer–seller relationships", Journal of Marketing, 1994, vol. 58: pp. 1–19.

[50] Geyskens, I., Steenkamp, J, and Kumar, N., "Generalizations about trust in marketing channel relationships using meta-analysis", International Journal of Research in Marketing, 1997, vol. 15: pp.223–248.

[51] Gill, J., and Butler, R., "Cycles of trust and distrust in joint-ventures", European Management Journal, 1996, vol. 14(1): pp. 81–89.

[52] Good, D., "Individuals, Interpersonal Relations, and Trust", in D. Gambetta (Eds.), Trust: Making and Breaking Cooperative Relations. University of Oxford Press, 2000.

[53] Golbeck, J., and Hendler, J., "Inferring reputation on the semantic web", Proceedings of the 13th International World Wide Web Conference, 2004.

[54] Grabner-Krauter, S., and Kaluscha, E., "Empirical Research in On-Line Trust: a Review and Critical

Assessment", International Journal of Human-Computer Studies, 2003, vol. 58: pp. 783-812.

[55] Granovetter, M., "The strength of weak ties", American Journal of Sociology, 1973, vol. 78: pp. 1360–1380.

[56] Granovetter, M., Getting a Job: A Study of Contacts and Careers. Harvard University Press, Harvard, 1974.

[57] Granovetter, M., "Economic Action and Social Structure: The Problem of Embeddedness", American Journal of Sociology, 1985, vol. 91(3): pp. 481–510.

[58] Granovetter, M., Society and Economy: The Social Construction of Economic Institutions. Harvard University Press, Harvard, 1991.

[59] Griffiths, N., Chao, K., and Younas, M., "Fuzzy Trust for Peer-to-Peer Systems", Proceedings of the 26th IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW'06), Portugal: Lisbon, 2006, 73-79.

[60] Gupta, M., Judge, P., and Ammar, M., "A reputation system for peer-to-peer networks", Proceedings of the 13th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV), 2003.

[61] Guth, W., "Do Banks Crowd in Business Ethics? An Indirect Evolutionary Analysis", International Review of Economics and Finance, 2001, vol. 10(1): pp. 1–17.

[62] Guth, W., and Kliemt, H., "Competition or co- operation on the evolutionary economics of trust exploitation and moral attitudes", Metroeconomica, 1994, vol. 45: pp. 155-187.

[63] Hardin, R., Trust and Trustworthiness. Russell Sage Foundation, 2002.

[64] Hart, O., "The theory of contracts", in: Bewley R. (Ed.), Advances in Economic Theory. Cambridge University Press, Cambridge, 1987.

[65] Hayek, F., Choice in Currency:A Way to Stop Inflation. The Institute of Economic Affairs, London, 1974.

[66] Hayek, F., Desnationalisation of Money: The Argument Redefined. The Institute of Economic Affairs, London, 1978.

[67] Hirshleifer, J., and Riley, J., "The Analytics of Uncertainty and Information: an Expository Survey", Journal of Economic Literature, 1979, vol. 17: pp. 1374–1421.

[68] Hume, D., A Treatise of Human Nature (1737). Clarendon Press: Oxford, 1975.

[69] Inkpen, A., and Currall, S., "The nature, antecedents, and consequences of joint venture trust", Journal of International Management, 1998, vol. 4(1): pp. 1–20.

[70] Jensen, M., and Meckling,W., "Theory of the firm: managerial behavior, agency cost, and ownership structure", Journal of Financial Economics, 1976, vol. 3(4): pp. 305-360.

[71] Jones, A., "On the concept of trust", Decision Support Systems, 2002, vol. 33: pp. 225–232.

[72] Josang, A., "Trust-based decision making for electronic transactions", Proceedings of the 4th Nordic Workshop on Secure Computer Systems (NORDSEC'99), Stockholm University, Sweden, 1999.

[73] Josang, A., "A logic for uncertain probabilities", International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2001, vol. 9(3): pp. 279– 311.

[74] Josang, A., and Ismail, R., "The beta reputation system", Proceedings of the 15th Bled Electronic Commerce Conference, Bled, Slovenia, 2002.

[75] Kamvar, S., Schlosser, M., and Garcia-Molina, H., "The Eigen-Trust algorithm for reputation management in P2P networks", Proceedings of the Twelfth International World Wide Web Conference, Budapest, 2003.

[76] Karlins, M., and Abelson, H., Persuasion, how opinion and attitudes are changed. Crosby Lockwood & Son, 1970.

[77] Klein, B., "The Competitive Supply of Money" Journal of Money Credit and Banking, 1974, November issue: pp. 423-53.

[78] Lahno, B., "On the Emotional Character of Trust", Ethical Theory and Moral Practice, 2001, vol. 4: pp. 171-189.

[79] Levien, R., Attack Resistant Trust Metrics, PhD thesis, University of California at Berkeley, 2004.

[80] Luhmann, N., Trust and Power. New York: Wiley, 1979.

[81] Luo, Y., "Building trust in cross-cultural collaborations: toward a contingency perspective", Journal of Management, 2002, vol. 28(5): pp. 669–694.

[82] Makino, J., "Productivity of research groups. Relation between citation analysis and reputation within research communities", Scientometrics, 1988, vol. 43(1): pp. 87– 93.

[83] Manchala, D., "Trust metrics, models and protocols for electronic commerce transactions", Proceedings of the 18th International Conference on Distributed Computing Systems, 1998.

[84] Marimon, R., Nicolini, J., and Teles, P., "Competition and Reputation", Proceedings of the World Conference Econometric Society, Seattle, 2000.

[85] Marsh, S., Formalising Trust as a Computational Concept. PhD thesis, University of Stirling, 1994.

[86] Maximilien, E., and Singh, M., "Agent Based Trust Model Involving Multiple Qualities", Proceedings of the 4th International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS'05), Netherlands: Utrecht, 2005, pp. 519-526.

[87] Mayer, R., Davis, J., and Schoorman, F., "An integrative model of organizational trust", Academy of Management Review, 1995, vol. 20(3): pp. 709–734.

[88] McKnight, D., and Chervany, N., "Notions of Reputation in Multi-Agent Systems: A Review", Proceedings of the 34th Hawaii International Conference on System Sciences, 2002a.

[89] McKnight, D., and Chervany, N., "What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology", International Journal of Electronic Commerce, 2002b, vol.6(2): pp. 35–59.

[90] McKnight, D., Cummings, L., and Chervany, N., "Initial trust formation in new organizational relationships", Academy of Management Review, 1998, vol. 23(3): pp. 473–490.

[91] Miller, N., Resnick, P., and Zeckhauser, R., "Eliciting Honest Feedback in Electronic Markets", Retrieved October 12, 2006 from http://www.si.umich.edu/presnick/papers/elicit/. Checked January 23, 2007.

[92] Morgan, R., and Hunt, S., "The commitment–trust theory of relationship marketing", Journal of

Marketing, 1994, vol. 58: pp. 20–38.

[93] Mui, L., Mohtashemi, M., and Ang, C., "A probabilistic rating framework for pervasive computing environments", Proceedings of the MIT Student Oxygen Workshop (SOW'2001), 2001.

[94] Mui, L., Halberstadt, A., and Mohtashemi, M., "Notions of reputation in multi-agent systems: a review", Proceedings of the first Int. Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS), 2002a.

[95] Mui, L., Mohtashemi, M., and Halberstadt, A., "A computational model of trust and reputation", Proceedings of the 35th Hawaii International Conference on System Science (HICSS), 2002b.

[96] Mui, L., Mohtashemi, M., Ang, C., Szolovits, P., and Halberstadt, A., "Ratings in Distributed Systems: a Bayesian Approach", Proceedings of the Workshop on Information Technologies and Systems (WITS), 2001.

[97] OnSale. http://www.onsale.com, 2002.

[98] Page, L., Brin, S., Motwani, R., and Winograd, T., The PageRank Citation Ranking: Bringing Order to the Web, Technical report, Stanford Digital Library Technologies Project, 1998.

[99] Pavlou, P., "Consumer Acceptance of Electronic Commerce — Integrating Trust and Risk with the Technology Acceptance Model", International Journal of Electronic Commerce, 2003, vol. 7(3): pp.69–103.

[100] Plato, The Republic (370BC). Viking Press, 1955.

[101] Resnick, P., Zeckhauser, R., Friedman, R., and Kuwabara, K., "Reputation systems", Communications of the ACM, 2000, vol. 43(12): pp. 45–48.

[102] Rockoff, H., The Free Banking Era: A Reconsideration. New York: Arno Press, 1975.

[103] Rotter, J., "A New Scale for the Measurement of Interpersonal Trust", Journal of Personality, 1967, vol. 35: pp. 651-665.

[104] Rotter, J., "Generalized Expectancies for Interpersonal Trust", American Psychologist, 1971, vol.26(5): pp. 443–452.

[105] Sabater, J., and Sierra, C., "REGRET: a reputation model for gregarious societies", Proceedings of the 4th Int. Workshop on Deception, Fraud and Trust in Agent Societies, in the 5th Int. Conference on Autonomous Agents (AGENTS'01), ACM Press, Montreal, Canada, 2001, pp. 61– 69.

[106] Sabater, J., and Sierra, C., "Reputation and social network analysis in multi-agent systems", Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS), 2002a.

[107] Sabater, J., and Sierra, C., "Social ReGreT, a reputation model based on social relations", SIGecom Exchanges, 2002b, vol. 3(1): pp. 44–56.

[108] Schillo, M., Funk, P., and Rovatsos, M., "Using Trust for Detecting Deceitful Agents in Artificial Societites", Applied Artificial Intelligence (Special Issue on Trust, Deception and Fraud in Agent Societies), 2000, pp. 825-848.

[109] Schneider, J. et al., "Disseminating trust information in wearable communities", Proceedings of the 2nd International Symposium on Handheld and Ubiquitous Computing (HUC2K), 2000.

[110] Sen, S., and Sajja, N., "Robustness of reputation-based trust: Boolean case", Proceedings of the First

International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS), 2002.

[111] Shankar, V., Sultan, F., Urban, G., and Bart, I., "The Role of Trust in Online Customer Support", Working Paper, Sloan School of Management, MIT, Cambridge, MA 02142, 2002.

[112] Shapiro, C., "Consumer information, product quality, and seller reputation", The Bell Journal of Economics, 1982, vol. 13(1): pp. 20– 35.

[113] Shapiro, C., "Premiums for high quality products as returns to reputations", Quarterly Journal of Economics, 1983, vol. 48: pp. 659-680.

[114] Shapiro, C., and Stiglitz, J., "Equilibrium unemployment as a worker discipline device", American Economic Review, 1984, vol. 74: pp. 433– 444.

[115] Stokey, N., "Credible Public Policy", Journal of Economic Dynamics and Control, 1991, vol. 15: pp. 627-656.

[116] Swan, J., Bowers, M., and Richardson, L., "Customer trust in the salesperson: an integrative review and meta-analysis of the empirical literature", Journal of Business Research, 1999, vol. 44: pp. 93–107.

[117] Sztompka, P., Trust: A Sociological Theory. Cambridge University Press, 1999.

[118] Tadelis, S., "Firm reputation with hidden information", Economic Theory, 2003, vol. 21(2): pp. 635–651.

[119] Taub, B., "Private Fiat Money with Many Suppliers", Journal of Monetary Economics, 1985, vol. 16:pp. 195–208.

[120] Taub, B., "Asymptotic Properties of Pipeline Control of the Money Supply", International Economic Review, 1986, vol. 27(3): pp. 647-665.

[121] Tomkins, C., "Interdependencies, Trust and Information in Relationships, Alliances and Networks", Accounting, Organizations and Society, 2001, vol. 26: pp.161–191.

[122] Wicks, A., Berman, S., and Jones, T., "The structure of optimal trust: moral and strategic implications", Academy of Management Review, 1999, vol. 24(1): pp. 99–116.

[123] Williamson, O., "Calculativeness, trust and economic organization", Journal of Law and Economics, 1993, vol. 36: pp. 453– 486.

[124] Withby, A., Josang, A., and Indulska, J., "Filtering out unfair ratings in Bayesian reputation systems", Proceedings of the 7th Int. Workshop on Trust in Agent Societies (at AAMAS'04), 2004.

[125] Yu, B., and Singh, M., "Towards a Probabilistic Model of Distributed Reputation Management",Proceedings of the Fourth Workshop on Deception, Fraud and Trust in Agent Societies, Montreal, Canada. 2001, pp. 125–137.

[126] Yu, B., and Singh, M., "An evidential model of distributed reputation management", Proceedings of the First Int. Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS), 2002.

[127] Zacharia, G., Moukas, A., and Maes, P., "Collaborative Reputation Mechanisms in Electronic Marketplaces", Proceedings of the 32nd Hawaii International Conference on System Science, IEEE, 1999.

[128] Ziegler, C., and Lausen, G., "Spreading activation models for trust propagation", Proceedings of the IEEE International Conference on e-Technology, e-Commerce, and e-Service (EEE '04), Taipei,

2004.

[129] Zucker, L., “Production of Trust: Institutional Sources of Economic Structure, 1840–1920”, Research in Organizational Behavior, 1986, vol. 6: pp. 53–111.

EFFECTIVE IMPLEMENTATION AND AVALANCHE EFFECT OF AES

Amish Kumar , Mrs. Namita Tiwari

Department of CSE MANIT-Bhopal

ABSTRACT

Efficient implementation of block cipher is critical towards achieving high efficiency with good understandability. Numerous number of block cipher including Advance Encryption Standard have been implemented using different platform. However the understanding of the AES algorithm step by step is very typical. This paper presents the efficient implementation of AES algorithm and explain Avalanche effect with the use of MATLAB platform. Mainly use of MATLAB in Algorithm development, Data analysis, exploration, visualization, modeling, simulation, prototyping, application development including GUI building and computation.

KEYWORDS

AES, Avalanche effect, S-Box.

For More Details:https://airccse.org/journal/ijsptm/papers/1213ijsptm03.pdf

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

REFERENCES

[1] Amish Kumar,Namita Tiwari, PERFORMANCE EVALUATION OF AES METHODS: REVIEW,ICCC 2012,paper id 1365

[2] Biham,Eli and Adi Shamir,Differential Cryptanalysis of the Data Encryption Standard, SpringerVerlag,1993.

[3] The Mathworks: Matlab,The Language of Technical Computing. http://www. mathworks.com/products/matlab,(2001).

[4] V.Rijmen: The block cipher Rijndael.http://www.esat.kuleuven.ac.be/rijmen/rijndael/,(2001).

[5] J.Daemen,V.Rijmen: AES proposal: Rijndael.http://www.esat.kuleuven.ac.be/~rijmen/rijndael/rijndaeldocV2.zip,(1999).

[6] National Institute of Standards and Technology: Specification for the Advanced Encryption Standard(AES). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf,(2001).

[7] National Institute of Standards and Technology: Data Encryption Standard (DES). http://csrc.nist.gov/publications/fips/fips46- 3/fips46-3.pdf,(2001).

[8] Radu Tomoiaga, Mircea Stratulat AES Performance Analysis on Several Programming Environments, Operating Systems or Computational Platforms", 2010 Fifth International Conference on Systems and Networks Communications.

[9] Chirag Parikh, M.S. Parimal Patel, Ph.D." Performance Evaluation of AES Algorithm on Various Development Platforms".

Authors

Amish Kumar,
M.Tech (Information security) NIT-Bhopal,
India

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.

AUTOMATED CONTROL FOR RISK ASSESSMENT ON UNIX OPERATING SYSTEM -I

[1]Dr. Prashant Kumar Patra & [2]Padma Lochan Pradhan

[1]Dept. of CSE, College of Engineering & Technology, BPUT, Bhubaneswar-751003
[2]Dept. of CSE, Sikha 'O' Anusandhan University. Bhubaneswar, Orissa, India

ABSTRACT

Control and Risk are the two parts of the coin. Risk management is the process of identifying vulnerabilities and threats to operating system resources to achieving business objectives and deciding what counter measures to take in reducing the lowest level of risk. The increased use of computer & communications system by IT industries has increased the risk of theft of proprietary information. Cryptographic control (Encryption) is a primary method of protecting system resources. Automated Control is probably the most important aspect of communications security and becoming increasingly important as basic building block for computer security. Automated Control is inversely proportional to the risk & mean while control is directly proportional to the quality of standard (S). Automated Control provides accountability for individuals who are accessing sensitive information on application, system software, server and network. This accountability is accomplished through access control mechanisms that require identification, authentication, authorization, non-repudiation, availability, reliability & integrity through the audit function. We have to develop java automated control for risk optimization based on unix operating system.

KEYWORDS

AC-Automated Control, PC- Preventive Control, SSH- Secure Shell, AES-Advance Encryption Standard, CBC: Cipher Block Chain, CERT-Computer Emergency Response Team, DC-Detective Control, CCCorrective Control, CMDB-Change Management Database, CKM-Cryptographic key management.

For More Details: https://airccse.org/journal/ijsptm/papers/2113ijsptm02.pdf

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

REFERENCES

[1] Bernard Kolman, Discrete Mathematical Structures Year 2007 5th Edn, PHI Chap 1, pp8-15

[2] Bookholdt, J. L. (1989) "Implementing Security and Integrity in Micro-Mainframe Networks,"MIS Quarterly (13) 2, pp. 135-144.

[3] Bruce Schneier, Applied Cryptography, Wiley 2nd Edition 1996 Chap7.1 pp-155

[4] CISA Review Mannual 2003, Chap 4, pp226-230

[5] Coriolis , CISSP Exam cram, dreamtech year 2002 (Chap 4 p 61-77)

[6] Edgar G, Discrete Mathematics with Graph Theory(2007), 3rd Edn pp57-58

[7] International Journal of Computer communication Technology (IJCCT Vol 1, Issue 1 Nov 2009 pp71

[8] International Journal of Computer Science &Tech(IJCST Vol 2, Issue 4 Oct-Dec 2011 pp22-27

[9] Joe. L Matt. Discrete Mathematics for Scientist and Mathematician(2008), PHI 2nd Edn Ch. P179.

[10] John B. Kramer, The CISA Prep Guide, Wiley Publishing Inc.Year 2003 Chap 7 pp420-450

[11] Mcl.ean, Kevin &Lenwatts(1996) Risk Analysis Methodology " IS audit & Control Journal III 32-36

[12] NIST special publication 800-30 Risk management guide for IS July 2002, page 8

[13] O' Reilly, Essentail of System Administration 1995 (Chap 10, P467- 485) & Chap 6(p201-243), Chap11

[14] Pressman, Software Engg 5th Edn, year 2001 MGH,Chap 6 (P 145- 162)

[15] Pichnarczyk, Karen, Weber, Steve & Feingold, Richard. "Unix Incident Guide: How to Detect an Intrusion CIAC-2305 R.1". C I A C Department of Energy. December,1994.

[16] Shon Harrish,CISSP Exam study guide, Dreamtech year 2002 DRP/BCP (Chap 9 P 591-603)

[17] Shon Harrish, Security Mgmt Practices, Wiley, Dreamtech CISSP Exam Year 2002 study guide 2003 (Chap 4 P 57-92)

[18] Sumitabh Das UNIX System V UNIX Concept & Application Chap 4-8.

[19] Sun-Microsystem UNIX sun solaris system administration: Vol 1 & Vol 2.

[20] William Stalling, Cryptography and Network Security(2006) 4th Edn Ch6.3 pp192 Ch9.2 pp-609-614

[21] Weber Ron , Information System audit & control PHI 2002(Chap 7 P- 243-285)

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 a nd 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.

CLOUD COMPUTING TECHNOLOGY: SECURITY ANDTRUST CHALLENGES

Sajjad Hashemi[1]

[1]Department of Computer Engineering, Science and Research Branch, Islamic Azad University, West Azarbayjan, Iran

ABSTRACT

A let of exclusive features such as high functionality and low cost have made cloud computing a valuable technology. These remarkable features give users and companies, countless opportunities to reach their goals spending minimum cost and time. Looking at the literature of this technology, it can be claimed that the main concerns of the users of cloud are security issues especially trust. Unfortunately these concerns have not been tackled yet. Therefore we decided to introduce a useful and functioned way to create more trust among consumers to use this technology .In this paper we suggest the foundation of an international certification institute for the service providing companies in order to increase trust and enhance likeliness of using this new and valuable technology among people. Practicality of the technology will improve it and will make its security better by providers.

KEYWORDS

Cloud Computer, Security, Trust

For More Details: https://airccse.org/journal/ijsptm/papers/2513ijsptm01.pdf

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

REFERENCES

[1] Yashpal Kadam, "Security Issues in Cloud Computing A Transparent View", International Journal of Computer Science & Emerging Technologies, Vol-2 No 5 October, 2011.

[2] Mohamed Al Morsy, John Grundy and Ingo Müller, "An Analysis of The Cloud Computing SecurityProblem", In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30 Nov 2010.

[3] H. Takabi, J.B.D. Joshi, G.Ahn., "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security Privacy Magazine, Vol 8, IEEE Computer Society, p.24-31, 2010.

[4] M. Monsef, N. Gidado, "Trust and privacy concern in the Cloud", 2011 European Cup, ISecurity for the Next Generation, p.1-15, 2011.

[5] M. Firdhous, O. Ghazali, and S. Hassan, Trust and Trust Management in Cloud Computing – A Survey, Inter Networks Research Group, University Utara Malaysia, Technical Report UUM/CAS/InterNetWorks/TR2011-01, 2011.

[6] Farhad SoleimanianGharehchopogh, Sajjad Hashemi, "Security Challenges in Cloud omputingwithmore Emphasis on Trust and Privacy", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, Vol. 1, ISSUE 6, pp. 49-54. 2012.

[7] D. Zissis, D. Lekkas, "Addressing cloud computing security issues", Future Generation Computer Systems, Volume 28, Issue 3, P. 583–592, March 2012.

[8] Mahbub Ahmed, Yang Xiang, Shawkat Ali, "Above the Trust and Security in Cloud Computing: A Notion towards Innovation", 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, pp.723-730, 2010.

[9] V.KRISHNA REDDY, Dr. L.S.S.REDDY, "Security Architecture of Cloud Computing", International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 9, pp.7149-7155, September 2011.

[10] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Elsevier, Network and Computer Applications, Vol. 34, p.1-11, 2010.

[11] K, Sachdeva, Cloud Computing: Security Risk Analysis and Recommendations, Master Thesis, University of Texas, Austin, 2011.

[12] Philipp Zech, "Risk–Based Security Testing in Cloud Computing Environments", 011 Fourth IEEE International Conference on Software Testing, Verification and Validation, pp.411-414, 2011.

[13] Fariborz farahmand, "Risk Perception and Trust in Cloud", ISACA JOURNAL VOLUME 4, pp.1-8, 2010.

[14] Hoover, J. N.; R. Martin; "Demystifying the Cloud," InformationWeek, June 2008.

[15] Weiss, A.; "Computing in the Clouds," netWorker, vol. 11, issue 4, p.16-25, 2007.

[16] D. Jamil, H. Zaki, Security Issues in Cloud Computing and Countermeasures, International Journal of Engineering Science and Technology, Vol. 3, No. 4, p. 2672-2676, 2011.

[17] S. Qaisar, K.F. Khawaja, Cloud Computing: Network/Security Threats and Countermeasures, Interdisciplinary journal of contemporary research in business, Vol.3, No 9, p. 1323-1329, 2012.

[18] J.R. Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics, Technical EditorBill Meine, Elsevier Publishing, 2011

[19] Siani Pearson, “Privacy, Security and Trust in Cloud Computing”, HP Laboratories, appeared as a book chapter by Springer, UK, 2012.

[20] Cloud Security Alliance (2009)” Security Guidance for Critical Areas of Focus in Cloud Computing”., v2.1, English language version, December. http://cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

[21] Vaquero L, Rodero-Merino L, Morán D, Locking the sky: a sur-vey on IaaS cloud security. Computing, 91:93–118, 2011.

[22] Jaeger PT, Fleischmann KR, Public libraries, values, trust, and e-government. In: Information Technology and Libraries, 26(4), 2007.

[23] Rousseau D, Sitkin S, Burt R, Camerer C, Not so Different after All: a Cross-discipline View of Trust. Academy of Management Re-view, 23(3):393-404, 1998.

[24] Wang Y, Lin K.-J, Reputation-Oriented Trustworthy Computing in E-Commerce Environments. Internet Computing, IEEE, 12(4):55–59, 2008.

[25] Singh S, Morley C, Young Australians’ privacy, security and trust in internet banking. In: Proceedings of the 21st Annual Conference of the Australian Computer-Human interaction Special interest Group: Design: Open 24/7, 2009.

[26] Osterwalder D, Trust Through Evaluation and Certification. So-cial Science Computer Review. Sage Publications, Inc., 19(1):32-46, 2005.

[27] Best SJ, Kreuger BS, Ladewig J, The effect of risk perceptions on online political participatory decisions. Journal of Information Tech-nology& Politics, 4, 2005.

[28] Nissenbaum H, Can Trust be Secured Online? A theoretical perspective. Etica e Politica, 2, 1999.

[29] Giff S, The Influence of Metaphor, Smart Cards and Interface Dialogue on Trust in eCommerce, MSc project, University College London, 2000.

[30] R.J.W. Welten (Rob). Towards the cloud-The role of trust and perceived privacy risk on the adoption of cloud computing, MasterThesis, Tilburg University, Netherlands, 2009.

[31] Pearson S, Casassa Mont M, Crane S, Persistent and Dynamic Trust: Analysis and the Related Impact of Trusted Platforms. In: Trust Management, Proc. iTrust 2005, LNCS 3477, Peter Herrmann, Valérie Issarny, Simon Shiu (eds), 355-363, 2005

.

Authors

Sajjad Hashemi is a M.Sc. student in Computer Engineering Department, Science and Research Branch, Islamic Azad University, West Azarbayjan, Iran.

Email: iau.hashemi@gmail.com

A PROVENANCE-POLICY BASED ACCESS CONTROL MODEL FOR DATA USAGE VALIDATION IN CLOUD

Muralikrishnan Ramane[1], Balaji Vasudevan[2] and Sathappan Allaphan[3]

[123]Department of Information Technology, University College of Engineering
Villupuram, Tamilnadu, India

ABSTRACT

In an organization specifically as virtual as cloud there is need for access control systems to constrain users direct or backhanded action that could lead to breach of security. In cloud, apart from owner access to confidential data the third party auditing and accounting is done which could stir up further data leaks. To control such data leaks and integrity, in past several security policies based on role, identity and user attributes were proposed and found ineffective since they depend on static policies which do not monitor data access and its origin. Provenance on the other hand tracks data usage and its origin which proves the authenticity of data. To employ provenance in a real time system like cloud, the service provider needs to store metadata on the subject of data alteration which is universally called as the Provenance Information. This paper presents a provenance-policy based access control model which is designed and integrated with the system that not only makes data auditable but also incorporates accountability for data alteration events.

KEYWORDS

Access Control, Provenance, Security Policy, Data Auditing

For More Details: https://airccse.org/journal/ijsptm/papers/3514ijsptm01.pdf

Volume Link: https://airccse.org/journal/ijsptm/vol3.html

REFERENCES

[1] Sundareswaran, Smitha, Anna Cinzia Squicciarini, and Dan Lin. "Ensuring distributed accountability for data sharing in the cloud." Dependable and Secure Computing, IEEE Transactions on 9, no. 4, 2012, pp. 556-568.

[2] Pearson, Siani, and Azzedine Benameur. "Privacy, security and trust issues arising from cloud computing." In Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on, pp. 693-702. IEEE, 2010

[3] R.K.L. Ko, B.S. Lee and S. Pearson, "Towards Achieving Accountability, Auditability and Trust in Cloud Computing," Proc. International workshop on Cloud Computing: Architecture, Algorithms and Applications (CloudComp2011), Springer, 2011, pp. 5.

[4] Sandhu, R. and Samarati, P, "Access control: Principles and practice," IEEE Communication Magazine (Sept.), 1994, pp. 40–48.

[5] P. Samarati and S.D.C. di Vimercati. "Access Control: Policies, Models, and Mechanisms," In FOSAD II, LNCS 2946, pp. 137–196.

[6] J. Park, D. Nguyen, and R. Sandhu, "A provenance-based access control model," In 10th Annual Conference on Privacy, Security and Trust, PST 2012. IEEE, July 2012.

[7] Park, Jaehong, Dang Nguyen, and Ravi Sandhu. "A provenance-based access control model." In Privacy, Security and Trust (PST), 2012 Tenth Annual International Conference on, IEEE, 2012, pp. 137-144.

[8] L. Popa, M. Yu, S. Ko, S. Ratnasamy, and I. Stoica, "CloudPolice: Taking access control out of the network," in Proc. of ACM HotNets, 2010.

[9] McDaniel, Patrick, Kevin RB Butler, Stephen E. McLaughlin, Radu Sion, Erez Zadok, and Marianne Winslett. "Towards a Secure and Efficient System for End-to-End Provenance." In TaPP. 2010.

[10] Sundareswaran, S. "Ensuring Distributed Accountability for Data Sharing in the Cloud," IEEE Transactions on Dependable and Secure Computing, Volume:9, Issue: 4, Aug. 2012, pp. 556- 568.

[11] T. Cadenhead, V. Khadilkar, M. Kantarcioglu, and B. Thuraisingham.A language for provenance access control. In Proceedings of the first ACM conference on Data and application security and privacy, ACM, 2011, pp. 133–144.

[12] Ni, Q. and Xu, S. and Bertino, E. and Sandhu, R. and Han, W., "An access control language for a general provenance model," Secure Data Management, Springer, 2009, pp.68–88.

AUTHORS

Muralikrishnan Ramane has completed post graduate degree in the field of Computer Science Engineering, specialized in Distributed Computing Systems. He is currently working as a Lecturer at University College of Engineering Villupuram, Tamilnadu, India. To his credit he has three International Journal and one International Conference publications. His research interests include Data Management in Distributed Environments.