December 2025: Top 10 Cited 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

OPTIMIZING IDENTITY MANAGEMENT: KEY STRATEGIES FOR EFFECTIVE GOVERNANCE AND ADMINISTRATION

Nikhil Ghadge

Software Architect, Workforce Identity Cloud, Okta.Inc

ABSTRACT

The significance of identity management has escalated in today's digital environment, where sensitive information is frequently at risk of breaches and unauthorized access. This research aims to investigate the best governance and administrative practices to enhance identity management systems, with a focus on security, privacy, and usability. By analyzing current industry standards, regulations, and technological advancements, the study intends to provide valuable insights for organizations seeking to improve their identity management capabilities. The research employs a mixed-methods approach, combining quantitative surveys and data analysis with qualitative interviews, to achieve a comprehensive understanding of current practices and challenges in identity governance and administration. Key components such as authentication, authorization, and access control are examined, with practical recommendations provided to enhance identity management strategies. The study emphasizes the importance of adopting role-based access control (RBAC), continuous monitoring and compliance, identity lifecycle management, and integrating identity governance with IT infrastructure. Additionally, it highlights the significance of effective password management, robust authentication measures, and the implementation of Single Sign-On (SSO) solutions to improve security and user experience. The research also underscores the critical role of data encryption and protection measures in safeguarding sensitive information and mitigating data breach risks. By adhering to best practices in identity management, organizations can strengthen their overall cybersecurity posture, ensure regulatory compliance, and build trust among stakeholders in an increasingly complex digital landscape.

KEYWORDS

Identity and Access Management, Digital Identity, Authentication, Authorization, Governance

For More Details: https://aircconline.com/ijsptm/V13N3/13324ijsptm01.pdf

Volume Link: https://airccse.org/journal/ijsptm/vol13.html

REFERENCES

[1] E. Bertino and Kenji Takahashi, Identity management : concepts, technologies, and systems. Boston: Artech House, 2011.

[2] N. Ghadge, "Enhancing Identity Management: Best Practices for Governance and Administration," in Computer Science & Information Technology (CS & IT), Jun. 2024, pp. 219–228. doi: https://doi.org/10.5121/csit.2024.141119.

[3] Chisita, Collence Takaingenhamo, Enakrire, Rexwhite Tega, Durodolu, Oluwole Olumide, Tsabedze, Vusi Wonderboy, and J. M. Ngoaketsi, Handbook of Research on Records and Information Management Strategies for Enhanced Knowledge Coordination. IGI Global, 2021.

[4] OECD, OECD Public Governance Reviews Kazakhstan: Review of the Central Administration. OECD Publishing, 2014.

[5] N. Ghadge, "Digital Identity in the Age of Cybersecurity: Challenges and Solutions," London Journal Of Research In Computer Science And Technology, vol. 24, no. 1.

[6] N. Ghadge, "Enhancing threat detection in Identity and Access Management (IAM) systems," International Journal of Science and Research Archive, vol. 11, no. 2, pp. 2050–2057, 2024, doi: https://doi.org/10.30574/ijsra.2024.11.2.0761.

[7] M. J. Haber and D. Rolls, Identity Attack Vectors. Apress, 2024.

[8] N. Ghadge, "Use Of Blockchain Technology To Strengthen Identity And Access Management (IAM)," International Journal of Information Technology (IJIT) , vol. 2, no. 2, pp. 1–17.

[9] S. K. Aikins, Managing E-Government Projects: Concepts, Issues, and Best Practices. IGI Global, 2012.

[10] C. Bartel, S. L. Blader, and A. Wrzesniewski, Identity and the modern organization. New York: Psychology Press, 2015.

[11] S. Katz et al., "Cultivating Wellbeing: Traditional Wisdom and Sustainability in Fiji's Green Schools," Proceedings of the Nutrition Society, vol. 83, no. OCE1, Apr. 2024, doi: https://doi.org/10.1017/s0029665124000259.

[12] A. Hashim, L. Van Jaarsveld, and B. Challens, "LEADERSHIP AND MANAGEMENT IN INTEGRATED MUSLIM SCHOOLS: A COMPLEX ENVIRONMENT." Accessed: Jun. 06, 2024. Online]. Available: https://endeducationconference.org/wpcontent/uploads/2023/06/02_OP_029.pdf

[13] Roberto Di Pietro, A. Colantonio, and A. Ocello, Role Mining In Business: Taming Role-based Access Control Administration. World Scientific, 2012.

[14] P. K. Goel, H. M. Pandey, A. Singhal, and S. Agarwal, Improving Security, Privacy, and Trust in Cloud Computing. IGI Global, 2024.

[15] E. Mccallister, T. Grance, K. Kent, and National Institute Of Standards And Technology (U.S, Guide to protecting the confidentiality of Personally Identifiable Information (PII) (draft) : recommendations of the National Institute of Standards and Technology. Gaithersburg, Md: U.S. Dept. Of Commerce, National Institute Of Standards And Technology, 2009.

ANALYSIS OF MEDIA DISCOURSE ON INTELLECTUAL PROPERTY RIGHTS RELATED TO METAVERSE IN KOREA

Ye-Sol Seo1, Hyo-Min Kim2 and Austin Kang3

1Department of Global Culture & Contents, Hankuk University of Foreign Studies
2Department of Korean and Chinese Culture, Hankuk University of Foreign Studies
3Department of Medicine, Seoul National University, Seoul, Republic of Korea

ABSTRACT

This study examines the evolving discourse on intellectual property rights (IPR) within the metaverse's Korean context, facilitated by the BIGKinds analytics program. As the metaverse transitions from a nascent concept to a complex reality, it reshapes digital interactions and poses new challenges for IPR, necessitating a comprehensive investigation into societal interest and legal discourse. The findings reveal a significant surge in metaverse-related IPR engagement over the past three years, aligning with the broader digital shift amid the COVID-19 pandemic. This pattern suggests an increasing need for nuanced legal approaches to copyright, trademark, and design patent protection in virtual environments. Thus, the urgency for legal reform to accommodate the metaverse's unique characteristics, the necessity for international collaboration on IPR in a borderless digital domain, and the intersection of technological advances, like NFTs and blockchain, with legal frameworks impacting creators' rights. As a result, this study provides policymakers and the digital community with real-time guidance on protecting intellectual property amid the transformative growth of the metaverse.

KEYWORDS

Metaverse, Intellectual property rights, BIGKinds, Discourse

For More Details: https://aircconline.com/ijsptm/V13N2/13224ijsptm01.pdf

Volume Link: https://airccse.org/journal/ijsptm/vol13.html

REFERENCES

[1] Hu, Y., & Liu, C. (2022). The 'metaverse society': Beyond the discourse intrinsic potential and transformative impact. Metaverse, Vol. 3, No. 2, p 14.

[2] Cheng, S. (2024). Applications of Web 3.0. InWeb 3.0: Concept, Content and Context(pp. 109-145). Singapore: Springer Nature Singapore.

[3] Mishra, S., Arora, H., Parakh, G., & Khandelwal, J. (2022, June). Contribution of blockchain in development of metaverse. In2022 7th international conference on communication and electronics systems (ICCES)(pp. 845-850). IEEE.

[4] Cheng, S. (2024). Applications of Web 3.0. InWeb 3.0: Concept, Content and Context(pp. 109-145). Singapore: Springer Nature Singapore.

[5] Aaron, L. S., & Roche, C. M. (2015). Intellectual Property Rights of Faculty in the Digital Age—Evolution or Dissolution in 21st Century Academia?.Journal of Educational Technology Systems, Vol. 43, No. 3, pp 320-341.

[6] Vig, S. (2022). Intellectual property rights and the metaverse: An Indian perspective. The Journal of World Intellectual Property, Vol. 25, No. 3, pp 753-766.

[7] Joy, A., Zhu, Y., Peña, C., & Brouard, M. (2022). Digital future of luxury brands: Metaverse, digital fashion, and non-fungible tokens. Strategic change, Vol. 31, No. 3, pp 337-343.

[8] Suzuki, S. N., Kanematsu, H., Barry, D. M., Ogawa, N., Yajima, K., Nakahira, K. T., ... & Yoshitake, M. (2020). Virtual Experiments in Metaverse and their Applications to Collaborative Projects: The framework and its significance. Procedia Computer Science, Vol.176, pp 2125-2132.

[9] Lee, D., & Kwon, H. (2022). Keyword analysis of the mass media's news articles on maker education in South Korea. International Journal of Technology and Design Education, Vol. 32, No.1, pp 333-353.

[10] Lee, S., Lee, J., Lee, J. M., Chun, H. W., & Yoon, J. (2023). A Network Analysis Approach to Detecting Social Issues with Web-Based Data. Applied Sciences, Vol.13, No.14, p 8516.

[11] Park, D., Kim, D., & Park, A. H. (2024). Agendas on Nursing in South Korea Media: Natural Language Processing and Network Analysis of News From 2005 to 2022. Journal of Medical Internet Research, Vol. 26, p e50518.

[12] Ritterbusch, G. D., & Teichmann, M. R. (2023). Defining the metaverse: A systematic literature review. Ieee Access, Vol. 11, p 12368-12377.

[13] Cheng-Han, T., & Kiat-Boon, D. S. (2023). The Metaverse beyond the internet. Law, Innovation and Technology, Vol.15, No. 2, pp 313-356.

[14] Koohang, A., Nord, J. H., Ooi, K. B., Tan, G. W. H., Al-Emran, M., Aw, E. C. X., ... & Wong, L. W. (2023). Shaping the metaverse into reality: a holistic multidisciplinary understanding of opportunities, challenges, and avenues for future investigation. Journal of Computer Information Systems, Vol. 63, No. 3, pp 735-765.

[15] Bibri, S. E., & Jagatheesaperumal, S. K. (2023). Harnessing the potential of the metaverse and artificial intelligence for the internet of city things: Cost-effective XReality and synergistic AIoT technologies. Smart Cities, 6(5), 2397-2429

[16] Jiang, Y., Kang, J., Niyato, D., Ge, X., Xiong, Z., Miao, C., & Shen, X. (2022). Reliable distributed computing for metaverse: A hierarchical game-theoretic approach. IEEE Transactions on Vehicular Technology, 72(1), 1084-1100.

[17] Hwang, G. J., & Chien, S. Y. (2022). Definition, roles, and potential research issues of the metaverse in education: An artificial intelligence perspective. Computers and Education: Artificial Intelligence, 3, 100082.

[18] Büchel, H., & Spinler, S. (2024). The impact of the metaverse on e-commerce business models–A delphi-based scenario study. Technology in Society, 102465.

[19] Onderdijk, K. E., Bouckaert, L., Van Dyck, E., & Maes, P. J. (2023). Concert experiences in virtual reality environments. Virtual Reality, Vol. 27, No.3, pp 2383-2396.

[20] Heo, J., Kim, D., Jeong, S. C., Kim, M., & Yoon, T. H. (2022). Examining Participant's perception of SPICE factors of metaverse MICE and its impact on Participant's loyalty and behavioral intentions. In Emotional Artificial Intelligence and Metaverse (pp. 183-197). Cham: Springer International Publishing.

[21] Belk, R., Humayun, M., & Brouard, M. (2022). Money, possessions, and ownership in the Metaverse: NFTs, cryptocurrencies, Web3 and Wild Markets. Journal of Business Research, Vol. 153, pp 198-205.

[22] Hosseini, S., Abbasi, A., Magalhaes, L. G., Fonseca, J. C., da Costa, N. M., Moreira, A. H., & Borges, J. (2024). Immersive Interaction in Digital Factory: Metaverse in Manufacturing. Procedia Computer Science, Vol. 232, pp 2310-2320.

[23] Allam, Z., Sharifi, A., Bibri, S. E., Jones, D. S., & Krogstie, J. (2022). The metaverse as a virtual form of smart cities: Opportunities and challenges for environmental, economic, and social sustainability in urban futures. Smart Cities, Vol.5, No.3, pp771-801.

[24] Seo, Y. S., & Kang, A. (2023). “Negative Attributes of the Metaverse Based on Thematic Analysis of Movie and .” International Journal of Computer Graphics & Animation, Vol.13, No.1, pp1-10.
[25] Romer, P. (2002). “When should we use intellectual property rights?” American Economic Review, Vol.92, No.2, pp 213-216.
[26] Kim, Y. K., Lee, K., Park, W. G., & Choo, K. (2012). Appropriate intellectual property protection and economic growth in countries at different levels of development. Research policy, Vol. 41, No.2, pp 358-375
[27] Gaikwad, A., & Dhokare, C. S. (2020). A Study of intellectual property rights and its significance for business. Journal of Information and Computational Science, Vol. 10, No. 2, pp 552-561.
[28] Yecies, B., Shim, A., Yang, J., & Zhong, P. Y. (2020). Global transcreators and the extension of the Korean webtoon IP-engine. Media, Culture & Society, Vol. 42, No.1, pp 40-57.
[29] Lee, K., Kim, J., Oh, J., & Park, K. H. (2013). Economics of intellectual property in the context of a shifting innovation paradigm: A review from the perspective of developing countries. Global Economic Review, Vol.42, No.1, pp 29-42.
[30] Kim, Y., Kim, D., Park, S., Kim, Y., Hong, J., Hong, S., ... & Oh, H. (2023). A Proposed Settlement and Distribution Structure for Music Royalties in Korea and Their Artificial Intelligence-Based Applications. Applied Sciences, Vol. 13, No.19, p 11109.
[31] Roh, T., Lee, K., & Yang, J. Y. (2021). How do intellectual property rights and government support drive a firm's green innovation? The mediating role of open innovation. Journal of Cleaner Production, Vol.317, p 128422.
[32] Kang, S., & Kim, S. (2022). Lessons Learned from Topic Modeling Analysis of COVID-19 News to Enrich Statistics Education in Korea. Sustainability, Vol.14, No. 6, p 3240.
[33] Bamakan, S. M. H., Nezhadsistani, N., Bodaghi, O., & Qu, Q. (2022). Patents and intellectual property assets as non-fungible tokens; key technologies and challenges. Scientific Reports, Vol. 12, No.1, p 2178.
[34] Lin, J., Long, W., Zhang, A., & Chai, Y. (2020). Blockchain and IoT-based architecture design for intellectual property protection. International Journal of Crowd Science, Vol.4, No.3, pp 283-293.
[35] Schultze, U. (2014). Performing embodied identity in virtual worlds. European Journal of Information Systems, Vol. 23, No.1, pp 84-95.
[36] Snowdon, D., Churchill, E. F., & Munro, A. J. (2001). Collaborative virtual environments: Digital spaces and places for CSCW: An introduction. In Collaborative virtual environments: Digital places and spaces for interaction (pp. 3-17). London: Springer London.
[37] Coleman, R., McCombs, M., Shaw, D., & Weaver, D. (2009). Agenda setting. InThe handbook of journalism studies (pp. 167-180). Routledge.

AUTHORS

The first author, **Ye-Sol Seo**, is affiliated with the Department of Global Culture & Contents at Hankuk University of Foreign Studies.

The second author, **Hyo-Min Kim**, is affiiliated with the Department of Korean and Chinese Culture at Hankuk University of Foreign Studies.

Austin Kang is the corresponding author and has been involved in numerous writing and academic activities.

TECHNICAL ANALYSIS ON THE CYBER ORGANIZATIONAL CRIMINOLOGY OF DICTATORIAL MILITARY CONDUCTS EXPERIENCE FROM HUMAN TRAFFICKING AND COERCIONS BY MILITARY CYBER AGGRESSIONS

Yang Pachankis

Ordained Minister, Universal Life Church, Modesto, CA, USA

ABSTRACT

The reformulated paper after the proceeding of the NCWMC 2022 recovers some previous manuscripts intercepted by the PLA of PRC for covert military operations with intrusions in global investment and financial systems. The crimes are analytically conducted through cloud servers and I/O for intelligence gathering. The information contained in the manuscripts with THEIR informatics not only could have led to further economic-financial surrogation of the PLA in American economy with investments, but also threats American national security through ontological calculation frameworks with artificial intelligence and further calculative power assertions - apart from the threats of outer space peace and security. It can be the reason behind the black hole and white hole observational results with the signal-satelliteinformation approach to general relativity manuscripts. A preliminary conception for defense strategy is proposed with previous insights and post facto security breaches to USA Space Command directly and national security conductively.

KEYWORDS

Space Command, National Security, Human Trafficking, Military Intelligence, Black Hole Information.

For More Details: https://aircconline.com/ijsptm/V11N3/11322ijsptm01.pdf

Volume Link: https://airccse.org/journal/ijsptm/vol11.html

REFERENCES

[1] Yang, Qiufen & Chen, Yuexin, (2001) "A Survey of the Ontology Methodology", Application Research of Computers, 2002, No. 4, pp. 5–7. http://www.cqvip.com/qk/93231x/2002004/6155383.html

[2] Pachankis, Yang, (2022) "Epistemological Extrapolation and Individually Targetable Mass Surveillance: The Issues of Democratic Formation and Knowledge Production by Dictatorial Controls", International Journal of Innovative Science and Research Technology, Vol. 7, Iss. 4, pp. 72–84. https://doi.org/10.5281/zenodo.6464858

[3] Xinhua Net, (2019) "中华人民共和国和俄罗斯联邦关于加强当代全球战略稳定的联合声明(全 文)", Xinhua News, 06-06-2019, Report Collection on Xi, Jinping.http://www.xinhuanet.com/world/2019-06/06/c_1124588720.htm

[4] Biddle, Tami Davis (2020) "Coercion Theory: A Basic Introduction for Practitioners", Texas: Texas National Security Review, Vol. 3, Iss. 2, pp. 94–109. http://dx.doi.org/10.26153/tsw/8864

[5] Pachankis, Yang (2022) "Targeted Human Trafficking - The Wars between Proxy and Surrogated Economy", International Journal of Scientific & Engineering Research, Vol. 13, Iss. 7, pp. 398–409.https://www.ijser.org/onlineResearchPaperViewer.aspx?Targeted_Human_Trafficking_The_Wars_between_Proxy_and_Surrogated_Economy.pdf

[6] Pachankis, Yang I. (2022) "Some Concepts of Space, Time, and Lengths in Simplified Chinese* - An Analytical Linguistics Approach", International Journal of Innovative Science and Research Technology, Vol. 7, Iss. 6, pp. 550–562. https://doi.org/10.5281/zenodo.6796083.

[7] Pachankis, Yang (2022) "Evidences on the PLA Interception in the Sciences for Covert Military Intelligence and Operations through Financial Operations", Zenodo. https://doi.org/10.5281/zenodo.6952516

[8] Pachankis, Yang, (2021) "Research on the Kerr-Newman Black Hole in M82 Confirms Black Hole and White Hole Thermonuclear Binding", Academia Letters, Article 3199. https://doi.org/10.20935/AL3199

[9] Pachankis, Yang I. (2022) "Physical Signals and their Thermonuclear Astrochemical Potentials: A Review on Outer Space Technologies", International Journal of Innovative Science and Research Technology, Vol. 7, Iss. 5, pp. 669-674. https://doi.org/10.5281/zenodo.6618334

[10] Pachankis, Yang Immanuel (2022) "White Hole Observation: An Experimental Result", International Journal of Innovative Science and Research Technology, Vol. 7, Iss. 2, pp. 779-790. https://doi.org/10.5281/zenodo.6360849

[11] Pachankis, Yang (2022) "Reading the Cold War through Outer Space: The Past and Future of Outer Space", International Journal of Scientific & Engineering Research, Vol. 13, Iss. 6, pp. 826-829. https://doi.org/10.14299/ijser.2022.06.03

[12] Pachankis, Yang (2022) "The Cultural Revisionist Element behind P. R. China's Neo-Nazism: A Cross-cultural and Cross-religion Research", International Journal of Advanced Multidisciplinary Research and Studies, Vol. 2, Iss. 4, pp. 435-451. https://doi.org/10.2139/ssrn.4163232

[13] Pachankis, Yang (2022) "MASS SURVEILLANCE, BEHAVIOURAL CONTROL, AND PSYCHOLOGICAL COERCION THE MORAL ETHICAL RISKS IN COMMERCIAL DEVICES", CS & IT – CSCP 2022, pp. 151-168.https://doi.org/10.5121/csit.2022.121313

[14] Stirone, Shannon (2018) "Welcome to the Center of the Universe", Longreads. https://longreads.com/2018/03/15/welcome-to-the-center-of-the-universe/

[15] Pachankis, Yang I. (2022) "White Hole Observation: An Experimental Result", Academia. https://www.academia.edu/video/1wAXok

[16] Pachankis, Yang Immanuel (2022) "A Multi-wavelength Data Analysis with Multi-mission Space Telescopes", International Journal of Innovative Science and Research Technology, Vol. 7, Iss. 1, pp. 701-708. https://doi.org/10.5281/zenodo.6044904

[17] Pachankis, Yang (2022) "The Modern Origin & Source of China's Techtransfer", International Journal of Scientific & Engineering Research, Vol. 13, Iss. 7, pp. 398–409. https://www.ijser.org/onlineResearchPaperViewer.aspx?Targeted_Human_Trafficking_The_Wars_between_Proxy_and_Surrogated_Economy.pdf

[18] Bertin, E. and Arnouts, S. (1996) "SExtractor: Software for source extraction", Astron. Astrophys., Suppl. Ser., Vol. 117, No. 2, pp. 393-404. https://doi.org/10.1051/aas:1996164

[19] Calabretta, M. R.and Greisen, E. W. (2002) "Representations of celestial coordinates in FITS",Astron. Astrophys., Vol. 395, No. 3, pp. 1077-1122.https://doi.org/10.1051/0004- 6361:20021327

[20] Greisen, E. W. and Calabretta, M. R. (2002) "Representations of world coordinates in FITS", Astron. Astrophys., Vol. 395, No. 3, pp. 1061-1075. https://doi.org/10.1051/0004-6361:20021326

[21] Greisen, E. W. and Calabretta, M. R. and Valdes, F. G. and Allen, S. L. (2006) "Representations of spectral coordinates in FITS", Astron. Astrophys., Vol. 446, No. 2, pp. 747-771. https://doi.org/10.1051/0004-6361:20053818

[22] Rots, Arnold H. and Bunclark, Peter S. and Calabretta, Mark R. and Allen, Steven L. and Manchester, Richard N. and Thompson, William T. (2015) "Representations of time coordinates in FITS - Time and relative dimension in space", Astron. Astrophys., Vol. 574, A36.https://doi.org/10.1051/0004-6361/201424653
[23] Joye, William (2019) "SAOImageDS9/SAOImageDS9 v8.0.1 (v8.0.1)", Zenodo. https://doi.org/10.5281/zenodo.2530958
[24] Krikke, Jan (2021) Leibniz, Einstein, and China, Olive Press.
[25] Mushakoji, Kinhide (1997) "Multilateralism in a Multicultural World: notes for a theory of occultation", in: Cox, Robert W. (eds) The New Realism, pp. 84-108. United Nations University Press. https://doi.org/10.1007/978-1-349-25303-6_5
[26] Wang, Hongying (1997) "Chinese Culture and Multilateralism", in: Cox, Robert W. (eds) The New Realism, pp. 145-161. United Nations University Press. https://doi.org/10.1007/978-1-349-25303-6_8
[27] Yuan, Jing-Dong (2007) "Culture matters: Chinese approaches to arms control and disarmament", Contemporary Security Policy, Vol. 19, Iss. 1, 85-128.https://doi.org/10.1080/13523269808404180
[28] Pachankis, Yang(2020) "Lateralism – The Globalization of US Hegemony after World War II", doctoral thesis, Communication University of China. https://www.ijser.org/thesis/yang_cao
[29] Poincaré, Henri(1907) The Value of Science, The Science Press.

AUTHORS

Yang Immanuel Pachankis is ordained by the Universal Life Church. He is granted Masters & PhD in Global Governance, Cosmology by research. He studied Directing (Editing Art & Technology) & Masters of Business Administration in Communication University of China

SECURITY AND PRIVACY PERCEPTIONS AMONG FEMALE ONLINE SOCIAL MEDIA USERS: A CASE STUDY OF BANGLADESH

Farida Chowdhury, Sadia Sultana and Mahruba Sharmin Chowdhury

Department of Computer Science and Engineering, Shahjalal University of Science and Technology, Bangladesh

ABSTRACT

Online Social Networks (OSNs) such as Facebook are extremely popular in Bangladesh, not only to the younger generations, but also to the people from other age categories as well. However, due to different socio-technological factors, the security and privacy awareness of Bangladeshi Facebook users have remained questionable. This is also evident in the wake of a number of incidents reported while using Facebook, particularly involving women users. There have been a few research studies to investigate different security and privacy concerns of Bangladeshi users. However, none of the existing has is comprehensive enough focusing only on female users. In this paper, we aim to fill in this gap by presenting a study on security and privacy concerns while using different Online Social Networks such as Facebook among female users in Bangladesh. We conducted an online survey of 203 Bangladeshi female Facebook users. We analyzed the survey statistics to study the general trend of behavior, practices, and expectations pertaining to secure Facebook usage and different privacy preferences. The study reveals that female users are concerned about their data privacy, however, 67% participants feel safe and secure while using Facebook and 33% participants do not think that Facebook takes necessary steps to protect users' data privacy on the web. We suggest that such a study can help researchers identify the privacy concerns in using social networking sites/apps such as Facebook to focus on building secure and privacy-friendly technologies to protect users from online crimes and harassment in developing countries.

KEYWORDS

Online Social Networks, Facebook, Security, Privacy, Survey

For More Details: https://aircconline.com/ijsptm/V10N1/10121ijsptm01.pdf

Volume Link: https://airccse.org/journal/ijsptm/vol10.html

REFERENCES

[1] NapoleonCat. (2020). "Facebook users in Bangladesh". Available online: https://napoleoncat.com/stats/facebook-users-in-bangladesh/2020/10

[2] Akter F. (2018). Cyber Violence against women: the case of Bangladesh. GenderIT.org. Available Online: https://www.genderit.org/articles/cyber-violence-against-women-case-bangladesh

[3] Ananthula S, Abuzaghleh O, Alla NB, Chaganti SB, Kaja PC, Mogilineedi D. (2015). "Measuring Privacy in Online Social Networks." International Journal of Security, Privacy and Trust Management (IJSPTM). 2015; 4(2):1-9.

[4] Ghazinour K, Matwin S, Sokolova M. (2013) "YourPrivacyProtector: A Recommender System for Privacy Settings in Social Networks." International Journal of Security, Privacy and Trust Management (IJSPTM). 2013; 2(4):11-25.

[5] Aldhafferi N, Watson C, Sajeev AS. (2013) "Personal Information Privacy Settings of Online Social Networks and their Suitability for Mobile Internet Devices." International Journal of Security, Privacy and Trust Management (IJSPTM). 2013; 2(2): 1-17.

[6] Ayaburi EW, Treku DN. (2020). "Effect of Penitence on Social Media Trust and Privacy Concerns: The Case of Facebook." International Journal of Information Management. 2020 Feb 1; 50:171-81.

[7] Jain R, Jain N, Nayyar A. (2020). "Security and Privacy in Social Networks: Data and Structural Anonymity." In Handbook of Computer Networks and Cyber Security 2020 (pp. 265-293). Springer, Cham.

[8] Rahaman A, and Ullah GM. (2013). "Exploration of Influencing Factors that Effecting Facebook Privacy Awareness on Bangladeshi Undergraduate University Students", available at SSRN 2592180 (2013).

[9] Ahmed S, Kabir A, Ahmed SS, and Jafrin S. (2017). "Cyber-crimes Against Womenfolk on Social Networks: Bangladesh Context." International Journal of Computer Applications 975 (2017): 8887.

[10] Sultana S, Saha P, Hasan S, Alam SMR, Akter R, Islam MM, Islam R, Al-Ameen MN, and Ahmed SI. (2020). "Understanding the Sensibility of Social Media Use and Privacy with Bangladeshi Facebook Group Users." In Proceedings of the 3rd ACM SIGCAS Conference on Computing and Sustainable Societies, pp. 317-318. 2020.

[11] Faruq MO, Rahman MM, and Alam MR. (2017). "Impact of Social Networking Sites in Bangladesh: Few Possible Solutions", International Journal of Intelligent Systems and Applications 9.4 (2017): 53.

[12] Moitra A, Hassan N, Mandal MK, Bhuiyan M, and Ahmed SA. (2020). "Understanding the Challenges for Bangladeshi Women to Participate in# MeToo Movement." Proceedings of the ACM on

[13] Human-Computer Interaction, no. 4 (GROUP): 1-25.

[14] Consumer Reports. (2012). "Protect your privacy on Facebook." Available Online: https://www.consumerreports.org/cro/2012/05/protect-your-privacy-on-facebook/index.html

[15] Natasha Stokes. (2020). "The Complete Guide to Facebook Privacy Settings", April 27, 2020. Available: https://www.techlicious.com/tip/complete-guide-to-facebook-privacy-settings/

[16] Chris Smith. (2019). "Facebook Privacy Settings: 18 changes you should make right away." 2019. Available: https://www.trustedreviews.com/news/facebook-privacy-settings-2939307

AUTHORS

Farida Chowdhury is an Associate Professor at the department of Computer Science and Engineering of the Shahjalal University of Science & Technology, Bangladesh. She received her PhD degree at the Institute of Computing Science and Mathematics at the University of Stirling, Scotland, UK. Her research interests focus on Network security, Security and Privacy, Security Usability, HCI, P2P networks, Pervasive computing and Social Networks.

Sadia Sultana is an Assistant Professor at the department of Computer Science and Engineering (CSE) of the Shahjalal University of Science and Technology (SUST), Bangladesh. She received her BSc Engineering and MSc degree from the same department. She was awarded Chancellor's Gold Medal for the outstanding result of her Bachelor degree. At the present, she is working as a PhD fellow at the department of CSE of SUST. Her research interests focus on Speech Analysis, Pattern Recognition, Artificial Intelligence, Data Mining, Distributed Computing and Social Computing.

Mahruba Sharmin Chowdhury received B.Sc honors degree in Computer Science and Engineering from Jahangirnagar University, Bangladesh in 2001. She worked as a software developer at a software company named Technohaven. Since 2004, she has been a faculty member at the department of Compute r Science and Engineering of the Shahjalal University of Science & Technology, Bangladesh. Her research interest includes Image Processing, Natural Language Processing, Network Security and Privacy, English to Bangla Conversion and Alignment.

VOICE BIOMETRIC IDENTITY AUTHENTICATION MODEL FOR IOT DEVICES

SalahaldeenDuraibi[1] , Frederick T. Sheldon[2] and Wasim Alhamdani[3]

[1]Computer Science Department University of Idaho Moscow, ID, 83844, USA
[1]Computer Science Department Jazan University Jazan, 45142, KSA
[2]Department of Computer Science University of Idaho, Coeur d'Alene, ID 83814, USA
[3]Department of Computer and Information Sciences, University of the Cumberlands, Williamsburg, KY, 40769, USA

ABSTRACT

Behavioral biometric authentication is considered as a promising approach to securing the internet of things (IoT) ecosystem. In this paper, we investigated the need and suitability of employing voice recognition systems in the user authentication of the IoT. Tools and techniques used in accomplishing voice recognition systems are reviewed, and their appropriateness to the IoT environment are discussed. In the end, a voice recognition system is proposed for IoT ecosystem user authentication. The proposed system has two phases. The first being the enrollment phase consisting of a pre-processing step where the noise is removed from the voice for the enrollment process, the feature extraction step where feature traits are extracted from user's voice, and the model training step where the voice model is trained for the IoT user. And the second being the phase verifies whether the identity claimer is the owner of the IoT device. Based on the resources limitedness of the IoT technologies, the suitability of text-dependent voice recognition systems is promoted. Likewise, the use of MFCC features is considered in the proposed system.

KEYWORDS

Internet of Things, Authentication, Access control, Biometric, Voice recognition, Security, Cybersecurity

For More Details: https://aircconline.com/ijsptm/V9N2/9220ijsptm01.pdf

Volume Link: http://airccse.org/journal/ijsptm/vol9.html

REFERENCES

[1] Olazabal, O., et al. Multimodal Biometrics for Enhanced IoT Security. in 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). 2019. IEEE.

[2] Ren, Y., et al., Replay attack detection based on distortion by loudspeaker for voice authentication. Multimedia Tools and Applications, 2019. 78(7): p. 8383-8396.

[3] Nainan, S. and V. Kulkarni. Performance evaluation of text independent automatic speaker recognition using VQ and GMM.in Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. 2016. ACM.

[4] McLaren, M., Automatic Speaker Recognition for Authenticating Users in the Internet of Things. August 26, 2016.

[5] Gupta, S. and S. Chatterjee, Text dependent voice based biometric authentication system using spectrum analysis and image acquisition, in Advances in Computer Science, Engineering & Applications. 2012, Springer. p. 61-70.

[6] Kolkata, C., About Voice biometric and Speaker Recognition. 2014.

[7] Thakur, A.S. and N. Sahayam, Speech recognition using euclidean distance. International Journal of Emerging Technology and Advanced Engineering, 2013. 3(3): p. 587-590.

[8] Petrovska-Delacrétaz, D., A. El Hannani, and G. Chollet, Text-independent speaker verification: state of the art and challenges, in Progress in nonlinear speech processing. 2007, Springer. p. 135-169.

[9] Rosenberg, A.E., F. Bimbot, and S. Parthasarathy, Overview of speaker recognition, in Springer Handbook of Speech Processing. 2008, Springer. p. 725-742.

[10] Yassine, A., et al., IoT big data analytics for smart homes with fog and cloud computing. Future Generation Computer Systems, 2019. 91: p. 563-573.

[11] Ferrag, M.A., L. Maglaras, and A. Derhab, Authentication and Authorization for Mobile IoT Devices Using Biofeatures: Recent Advances and Future Trends. Security and Communication Networks, 2019. 2019.

[12] Hamidi, H., An approach to develop the smart health using Internet of Things and authentication based on biometric technology. Future generation computer systems, 2019. 91: p. 434-449.

[13] Reynolds, D.A., T.F. Quatieri, and R.B. Dunn, Speaker verification using adapted Gaussian mixture models. Digital signal processing, 2000. 10(1-3): p. 19-41.

[14] Su, X., et al., Study to improve security for IoT smart device controller: drawbacks and countermeasures. Security and Communication Networks, 2018. 2018.

[15] Li, D., J. Wang, and Y. Yang. PVD: A new pathological voice dataset for intra-speaker recognition research interest. in 2016 10th International Symposium on Chinese Spoken Language Processing (ISCSLP). 2016. IEEE.

[16] Zhang, X., et al. Single Biometric Recognition Research: A Summary. in Proceedings of the 6th International Conference on Information Technology: IoT and Smart City. 2018. ACM.

[17] Brunet, K., et al. Speaker recognition for mobile user authentication: An android solution. 2013.

[18] Gofman, M., et al. Multimodal biometrics via discriminant correlation analysis on mobile devices. in Proceedings of the International Conference on Security and Management (SAM). 2018. The Steering Committee of The World Congress in Computer Science, Computer.

[19] Gbadamosi, L., Voice Recognition System Using Template Matching. International Journal of Research in Computer Science, 2013. 3(5): p. 13.

[20] Thullier, F., B. Bouchard, and B.-A. Menelas, A Text-Independent Speaker Authentication System for Mobile Devices. Cryptography, 2017. 1(3): p. 16.

[21] Anwar, M.U., Design of an enhanced speech authentication system over mobile devices. 2018.

[22] Khitrov, A. and K. Simonchik, System for text-dependent speaker recognition and method thereof. 2019, Google Patents.

[23] Oak, R., A Literature Survey on Authentication Using Behavioural Biometric Techniques, in Intelligent Computing and Information and Communication. 2018, Springer. p. 173-181.

[24] Khamis, M., et al. Gazetouchpass: Multimodal authentication using gaze and touch on mobile devices. in Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems. 2016.

[25] Arteaga-Falconi, J.S., H. Al Osman, and A. El Saddik, ECG authentication for mobile devices. IEEE Transactions on Instrumentation and Measurement, 2015. 65(3): p. 591-600.

[26] Shahzad, M., A.X. Liu, and A. Samuel, Behavior based human authentication on touch screen devices using gestures and signatures. IEEE Transactions on Mobile Computing, 2016. 16(10): p. 2726-2741.

[27] Ali, Z., et al., Edge-centric multimodal authentication system using encrypted biometric templates. Future Generation Computer Systems, 2018. 85: p. 76-87.

[28] Frank, M., et al., Touchalytics: On the applicability of touchscreen input as a behavioral biometric for

continuous authentication. IEEE transactions on information forensics and security, 2012. 8(1): p. 136-148.
[29] Tasia, C.J., et al., Two novel biometric features in keystroke dynamics authentication systems for touch screen devices. Security and Communication Networks, 2014. 7(4): p. 750-758.
[30] Khan, M.K., S. Kumari, and M.K. Gupta, More efficient key-hash based fingerprint remote authentication scheme using mobile device. Computing, 2014. 96(9): p. 793-816.
[31] Mahbub, U., et al. Partial face detection for continuous authentication. in 2016 IEEE International Conference on Image Processing (ICIP). 2016. IEEE.
[32] De Marsico, M., et al., Firme: Face and iris recognition for mobile engagement. Image and Vision Computing, 2014. 32(12): p. 1161-1172.
[33] Shin, D.-G. and M.-S. Jun. Home IoT device certification through speaker recognition.in 2015 17th International Conference on Advanced Communication Technology (ICACT). 2015. IEEE.
[34] Atwady, Y. and M. Hammoudeh. A survey on authentication techniques for the internet of things.in Proceedings of the International Conference on Future Networks and Distributed Systems. 2017. ACM.
[35] Sahoo, T.R. and S. Patra, Silence Removal and Endpoint Detection of Speech Signal for Text Independent Speaker Identification. International Journal of Image, Graphics & Signal Processing, 2014.6(6).
[36] Zhang, X., et al. Voice Biometric Identity Authentication System Based on Android Smart Phone. in 2018 IEEE 4th International Conference on Computer and Communications (ICCC). 2018. IEEE.
[37] Moussa, A.N., N.B. Ithnin, and O.A. Miaikil. Conceptual forensic readiness framework for infrastructure as a service consumers. in 2014 IEEE Conference on Systems, Process and Control (ICSPC 2014). 2014. IEEE.
[38] Dhakal, P., et al., A Near Real-Time Automatic Speaker Recognition Architecture for Voice-Based User Interface. Machine Learning and Knowledge Extraction, 2019. 1(1): p. 504-520.
[39] Moussa, A.N., et al. A Consumer-Oriented Cloud Forensic Process Model.in 2019 IEEE 10th Control and System Graduate Research Colloquium (ICSGRC). 2019. IEEE.
[40] Moussa, A.N., N. Ithnin, and A. Zainal, CFaaS: bilaterally agreed evidence collection. Journal of Cloud Computing, 2018. 7(1): p. 1.

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.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.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.ht

[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.

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

AUTHORS

Geetha Mahadevaiah, (Corresponding Author) Senior Director at Philips, Research Department, PIC, Bangalore.30+ years of experience in software engineering and management. Areas of intere st : Clinical decision support systems, Semantic Web, healthcare applications Bachelor of Engineering in Computer Scien ce 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.

A METHOD OF TRUST MANAGEMENT IN WIRELESS SENSOR NETWORKS

Janusz Górski and Alan Turower

Department of Software Engineering, Gdańsk University of Technology, Gdańsk, Poland

ABSTRACT

The research problem considered in this paper is how to protect wireless sensor networks (WSN) against cyber-threats by applying trust management and how to strengthen network resilience to attacks targeting the trust management mechanism itself. A new method, called WSN Cooperative Trust Management Method (WCT2M), of distributed trust management in multi-layer wireless sensor networks is proposed and its performance is evaluated. The method is specified by giving its class model in UML and by explaining the related attributes and methods. Different attacks against the network and against WCT2M deployed in the network are considered. The experimental evaluation of WCT2M involves laboratory experiments and simulations using a dedicated simulator. The evaluation focuses on efficiency of detecting and isolating the malicious nodes that implement different attack scenarios in the network and on the method's sensitivity to the changes in effectiveness of the security mechanisms deployed in the network nodes.

KEYWORDS

Wireless Sensor Network; trust management; security threat; attack scenario; simulation

For More Details: https://aircconline.com/ijsptm/V7N4/7418ijsptm01.pdf

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

REFERENCES

[1] Y. Zhiyng, K. Daeyoung, L. Insun, K. Kiyoung and J. Jongsoo, "A Security Framework with Trust Management for Sensor Networks," in Proc. Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, Athens, IEEE, 2005, pp. 184- 192.

[2] ZigBee Alliance, "Standards: ZigBee Specification," 28 01 2017. [Online]. Available: http://www.zigbee.org/download/standards-zigbee-specification/. [Accessed 05 11 2017].

[3] IEEE, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)," IEEE Press, New York, 2003.

[4] ANGEL, "Description of Final Angel Demonstrator," 6th FR STREP Project: Advanced Networked embedded platform as a Gateway to Enhance quality of Life (ANGEL), Deliverable 5.2, 2008.

[5] A. Keshavarzian, H. Lee and L. Venkatraman, "Wakeup Scheduling in Wireless Sensor Networks," in Proceeding of the 7th ACM International Symposium on Mobile ad hoc networking and computing, Florence, Italy, ACM, 2006, pp. 322-333.

[6] J. Górski and A. Turower, "Assessing the time effectiveness of trust management in fully synchronised wireless sensor networks," in Design, development and implementation of real-time systems; Trybus L. & Mastalerz M.W. (eds), Szczecin, Poland, PTI, 2013, pp. 31-42.

[7] N. I. Blatt, "Operational Trust: A New Look at the Human Requirement in Network Centric Warfare," in 9th International Command and Control Research and Technology Symposium (ICCRTS): Coalition Transformation: An Evolution of People, Processes and Technology to Enhance Interoperability; Leoni Warne (ed), Copenhagen, Danmark, Command and Control Research Program (US), 2004, pp. 1-17.

[8] J. Górski, A. Turower and A. Wardziński, "Distributed Trust Management Model for Wireless Sensor Networks," in Monographs of system dependability: Problems of dependability and modelling; Mazurkiewicz J., Sugier J., Walkowiak T. & Michalska K. (eds), Wrocław, Poland, Oficyna WYdawnicza Politechniki Wrocławskiej, 2011, pp. 83-94.

[9] T. Zahariadis, H. C. Leligou, P. Trakadas and S. Voliotis, "Trust management in wireless sensor networks," Transactions on Emerging Telecommunications Technologies, vol. 21, pp. 386-395, 2010.

[10] Y. Yu, K. Li, W. Zhou and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," Journal of Network and Computer Applications, vol. 35, vol. 35, pp. 867-880, 2012.

[11] J. Lopez, R. Roman, I. Agudo and C. Fernandez-Gago, "Trust management systems for wireless sensor networks: Best practices," Journal of Network and Computer Applications, vol. 35, vol. 33, pp. 1086-1093, 2010.

[12] F. Buccafurri, L. Coppolino, S. D'Antonio, A. Garofalo, G. Lax, A. Nocera and L. Romano, "TrustBased Intrusion Tolerant Routing in Wireless Sensor Networks," in Computer Safety, Reliability, and Security. SAFECOMP 2014, Lecture Notes in Computer Science; Bondavalli A., Di Giandomenico F. (eds), vol. 1, Florence, Italy, Springer, 2014, pp. 214-229.

[13] R. Abassi and S. G. El Fatmi, "Countering the Collusion Attack in a Trust-based MANET," in Proceedings of the European, Mediterranean & Middle Eastern Conference on Information Systems 2015; Kostantinos Lambrinoudakis, Vincenzo Morabito & Marinos Themistocleous (eds)., vol. 1, Athens, Greece, 2015, pp. 575-585.

[14] R. Perlman, "An overview of PKI trust models," IEEE Network, vol. 36, vol. 13, no. 6, pp. 38-43, 1999.

[15] H. Chen, H. Wu, X. Zhou and C. Gao, "Agent-based Trust Model in Wireless Sensor Networks," in Proc. International Conference on Multimedia and Ubiquitous Engineering, Busan, Korea, IEEE, 2008, pp. 150-154.

[16] H. Chen, H. Wu, X. Zhou and C. Gao, "Reputation-based Trust in Wireless Sensor Networks," in Proc. International Conference on Multimedia and Ubiquitous Engineering, Seoul, Korea, IEEE, 2007, pp. 603-607.

[17] A. Boukerche and X. Li, "An Agent-based Trust and Reputation Management Scheme for Wireless Sensor Networks," in Proc. IEEE Global Telecommunications Conference, St. Louis, USA, IEEE, 2005, pp. 1857-1861.

[18] J. Konorski and R. Orlikowski, "DST-Based Detection of Non-cooperative Forwarding Behavior of MANET and WSN Nodes," in ireless and Mobile Networking. IFIP Advances in Information and Communication Technology, vol 308, Berlin, Springer, 2009, pp. 185-196.

[19] [N. Labraoui, "A reliable trust management scheme in wireless sensor networks," in 12th International Symposium on Programming and Systems, Algiers, Algeria, IEEE, 2015, pp. 1-6.

[20] W. Fang, W. Zhang, Y. Yang, Y. Liu and W. Chen, "A resilient trust management scheme for defending against reputation time-varying attacks based on BETA distribution," Science China Information Sciences, vol. 60, no. 4, pp. 1-11, 2017.

[21] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," in First IEEE International Workshop on Sensor Network Protocols and Applications (SNPA 03),

Anchorage, Alaska, IEEE, 2003, pp. 113-127.
[22] Y. Sun, Z. Han and K. Liu, "Defense of Trust Management Vulnerabilities in Distributed Networks," Communications Magazine, vol. 46, no. 46, pp. 112-119, 31 March 2008.
[23] B. Mamalis, D. Gavalas, C. Konstantopoulos and G. Pantziou, "Clustering in Wireless Sensor Networks," in RFID and Sensor Networks: Architectures, Protocols, Security, and Integrations, L. Y. Y. Zhang (ed.), CRC Press, 2009, pp. 324-353.
[24] Texas Instruments, "CC2520 Development Kit," 10 07 2017. [Online]. Available: http://www.ti.com/tool/cc2520dk. [Accessed 05 11 2017].
[25] NetBeans, "NetBeans IDE Features," 10 07 2017. [Online]. Available: https://netbeans.org/features/index.html. [Accessed 05 11 2017].
[26] Java, "Java," 10 07 2017. [Online]. Available: http://www.java.com. [Accessed 05 11 2017].
[27] JGraph Ltd, "JGraph," 10 07 2017. [Online]. Available: http://www.jgraph.com/. [Accessed 05 11 2017].
[28] R. van Solingen and E. Berghout, The Goal/Question/Metric method: A practical guide for quality improvement of software development, McGraw-Hill Publishing Company, 1999.
[29] A. Turower, "Trust Management Method for Wireless Sensor Networks (Doctoral dissertation)," 2017. [Online]. Available: https://mostwiedzy.pl/publication/download/1/trust-management-methodfor-wireless-sensor-networks_16168.pdf. [Accessed 5 11 2017].
[30] E. Bulut, Z. Wang and B. K. Szymanski, "The Effect of Neighbor Graph Connectivity on Coverage Redundancy in Wireless Sensor Networks," Communications (ICC), 2010 IEEE International Conference on, pp. 1 - 5, 2010.
[31] F. Delicato, F. Protti, J. F. De Rezende, L. Rust and L. Pirmez, "Application-driven node management in multihop wireless sensor networks," Lecture Notes in Computer Science, pp. 569-576, 2005.
[32] A. Jhumka and L. Mottola, "On Consistent Neighborhood Views in Wireless Sensor Networks," Reliable Distributed Systems, 2009. SRDS '09. 28th IEEE International Symposium on, pp. 199 - 208, 2009.
[33] W. Ye, J. Heidemann and D. Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks," in Proc. INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, New York, USA, IEEE, 2002, pp. 1567-1576. [2] Gizem, Aksahya & Ayese, Ozcan (2009) Coomunications & Networks, Network Books, ABC Publishers.

AUTHORS

Janusz Górski is a professor at the Department of Software Engineering, Gdansk University of Technology in Poland where he is leading the Information Assurance Group (IAG) http://iag.pg.gda.pl/iag/.

Alan Turower is presently a cloud software developer and a design lead at Intel Technology Poland company.

PERUSAL OF INTRUSION DETECTION AND PREVENTION SYSTEM ON A MANET WITH BLACK HOLE ATTACK:ISSUES AND CHALLENGES

Marepalli Radha[1] and C.V.Guru Rao[2]

[1]Department of computer science and engineering, Adam"s college, Paloncha, Telangana, India
[2]SR Enginnering College, Warangal, Telangana, India

ABSTRACT

MANET is a self configuring network of nodes which is a wireless . The nodes in this network move randomly .Mobility of nodes is more. The nodes are dynamic and infrastructure less ,self maintainable. In MANET there are many types of security attacks like Blackhole, greyhole attack, wormhole, jellyfish etc. When the MANET is under blackhole attack there is a loss of energy which is high at the node resulting in loss of battery backup and also excess of bandwidth may be consumed by the attacker. The attacker is an insider. Among various mobility models to generate mobility patterns the Random waypoint mobility model is used .To solve these issues an IDPS framework for MANET using image processing techniques under blackhole attack is proposed to detect the blackhole attack RREP by providing security services like authentication and confidentiality.

KEYWORDS

AODV, BLACKHOLE ATTACK, IDPS, MANET, RWM IMAGE PROCESSING.

For More Details: https://aircconline.com/ijsptm/V7N2/7218ijsptm01.pdf

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

REFERENCES

[1] Ankur O. Bangand Prabhakar L. Ramteke. 2013. MANET: History,Challenges And Application International Journal of Application or Innovation in Engineering & Management Vol.2 Issue 9.

[2] V.G.Muralishankar and Dr. E. George Dharma Prakash Raj. 2014 Routing Protocols for MANET: A Literature Survey. International Journal of Computer Science and Mobile Applications Vol.2 Issue pg. 18-24

[3] parvinder Kaur, Dr. Dalveer Kaur & Dr. Rajiv Mahajan. 2015. The Literature Survey on Manet Routing Protocols and Metrics. Global Journal of Computer Science and Technology Volume 15 Issue 1 Version 1.0

[4] Bilal Maqbool Beigh , Uzair Bashir and Manzoor Chachoo . 2013. Intrusion Detection and Prevention System: Issues and Challenges.International Journal of Computer Applications (0975 – 8887) Volume76 No.17.

[5] Muhammad Amir Nisar, Amir Mehmood and Adnan Nadeem. 2013 A Review and Performance Analysis of Mobility Models for MANETs: A Case Study. Federal Urdu University of Arts Science & Technology, Karachi, Pakistan, Conference Paper.

[6] M. Sandhya Rani, R .Rekha, K.V.N.Sunitha, Performance Evaluation of MANET Routing Protocols Using Random Waypoint Mobility Model. International Journal of Advanced Research in Computer Science and Software Engineering 4(4), April - 2014, pp. 1293-1299

[7] AnuBala, Jagpreet Singh and MunishBansal “Performance Analysis of MANET under Blackhole Attack” First International Conference on Network and Communication 2009

[8] Bilal Maqbool Beigh , Uzair Bashir and Manzoor Chachoo . 2013. Intrusion Detection and Prevention System: Issues and Challenges.International Journal of Computer Applications (0975 – 8887) Volume76 No.17.

[9] Jeoren Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demester “ An Overview of Mobile ad hoc Netwroks: Applications &Challenges .“

[10] C.E. Perkins, E.M. Royer, S.R. Das, Ad hoc on demand distance vector (AODV) routing, in: IEEE WMCSA, 1999

[11] M. Medadian, A. Mebadi and E. Shahri: "Combat with black hole attack in AODV routing protocol",Proceedings of the 9th IEEE Malaysia International Conference on Communications (MICC), pp. 530-535, 2009

[12] Vani and D. S. Rao: "Removal of blackhole attack in ad hoc wireless networks to provide confidentiality security service", International Journal of Engineering Science and Technology,Vol. 3, pp.2377-2384, 2011.

[13] P. K. Singh and G. Sharma: "An efficient prevention of black hole problem in AODV routing protocol in MANET", Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications(TrustCom), pp. 902-906, 2012.

[14] M. K. J. Kumar and R. S. Rajesh: "Performance Analysis of MANET Routing Protocols in Different Mobility Models", IJCSNS International Journal of Computer Science and Network Security, Vol. 9 No.2, pp. 22-29, 2009.

[15] Muhammad Amir Nisar, Amir Mehmood and Adnan Nadeem. 2013 A Review and Performance Analysis of Mobility Models for MANETs: A Case Study. Federal Urdu

[16] Dr. A. Francis Saviour Devaraj , Mr. Akalu Assefa , TO PROPOSE A FRAMEWORK – IDPS FOR A MANET UNDER FLOODING ATTACK, JournalOf Advanced Research in Engineering & Management (IJAREM)ISSN: 2456-2033 || PP. 34-44

[17] B. Zhang H.T. Mouftah "QoS Routing for Wireless Ad Hoc Networks: Problems Algorithms and Protocols" IEEE Communications Magazine vol. 43 no. 10 pp. 110-117 Oct. 2005.

[18] Ravi Kant, Sunil Gupta, A Literature Survey on Black Hole Attacks on AODV Protocol in MANET, International Journal of Computer Applications (0975 – 8887) Volume 80 – No 16, October 2013

[19] SaritaBadiwal, AishwaryKulshrestha, NeerajGarg, Analysis of Black Hole Attack in MANET using AODV Routing Protocol, International Journal of Computer Applications (0975 –8887)Volume 168 – No.8, June 2017

[20] Prof.M.B.Lonare1, Anil Choudhary2, Chehel Sharma3, Ershad Mulani4, Harish Yadav5, Prevention and Detection of Blackhole Attack in MANET using Modified AODV Protocol, International Journal of Advance Engineering and Research Development Volume 4, Issue 4, April -2017

[21] Q. Xiao, “A biometric authentication approach for high security ad-hocnetworks,” in Proc. IEEE Info. Assurance Workshop, West Point, NY,June 2004.

[22] Ross and A. K. Jain, “Multimodal biometrics: an overview,” in Proc.12th European Signal Proc. Conf., Vienna, Austria, 2004.

[23] Ross and A. K. Jain, “Information fusion in biometrics,” Pattern Recognition Lett., vol. 24, pp. 2115-

2225, Sept. 2003.
[24] C.E. Perkins, E. M. Belding-Royer, and S. R.Das, “AdHoc On-Demand Distance Vector Routing”, IETF RFC 3561,July 2003.
[25] M.Ambika , R.V.Natraj Intrusion Detection and Continuous Authentication using Multimodal Biometrics in MANETS – A Survey, International Journal of Computer Applications (0975 – 8887) International Conference on Innovations In Intelligent Instrumentation, Optimization And Signal Processing “ICIIIOSP-2013”
[26] S. Bu, F. Yu, X. Liu, P. Mason and H. Tang, “Distributedcombined authentication and intrusion detection with data fusionin high-security mobile ad hoc networks,” IEEE Transactions onVehicular Technology, vol 60 no.3 pp. 1025–1036, March 2011.
[27] H.Nakayama, S.Kurosawa, A.Jamalipour, Y. Nemoto, N.Kato, "A Dynamic Anomaly Detection Scheme for AODVBasedMobile Ad Hoc Networks," IEEE Transactions onVehicular Technology, vol.58, no.5, pp.2471-2481, Jun 2009
[28] Sim T, Zhang S, R.Janakiraman and S.Kumar, “Continuous verification using multimodal biometrics,” IEEE Trans. Pattern Anal. Mach. Intell.2007; vol. 29, pp. 687-700.
[29] Korman J, A C Morris, D Wu and S.A.Jassim, “Multi-modal biometrics authentication on the secure phone PDA,” in Proc. 2nd Workshop Multimo
[30] Hiteishi Diwanji and J.S. Shah. “Enhancing Security in MANET through Unimodal Biometric Encryption Key” in IEEE, December 2011.

AUTHORS DETAILS:

M.Radha is currently Working as a Associate professor for 15 years She received her B.Tech degree from Swami Ramanadha institute of scince and technology ,Nalgonda and M.Tech degree from Karshak Engineering college ,Hyderabad in 2009.Her research lies in the field of wireless networking especially in MANET.

Dr.C.V.Guru Rao working as a professor Director over a period of 32 years in his Service. He was awa rded Ph.D degree in Computer science and Engineering from Indian Institute of Technology, Kharagpur, west Bengal, India.

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.

LOCATION PRIVACY ONLINE: CHINA, THE NETHERLANDS AND SOUTH KOREA

Peter Broeder[1] and Yujin Lee[2]

[1]Communication and Information Sciences, Tilburg University, The Netherlands
[2]Research Instruments, Falmouth, United Kingdom

ABSTRACT

The aim of the study is to explore cross-cultural differences in users' location privacy behaviour on LBSNs (location-based social networks) in China, the Netherlands and Korea. The study suggests evidence that Chinese, Dutch and Korean users exhibit different location privacy concerns, attitudes to social influence, perceived privacy control and willingness to share location-related information on LBSNs. The results show that in general, the more concerned users are about location privacy, the less they are willing to share and it also suggests that location privacy concern and social influence affect each other. Furthermore, the more control people perceive they have over their privacy, the more they are willing to share location information. A negative relationship between willingness to share location information and users' actual sharing of location information was seen. In short, it is concluded that the relation between cultural values and location privacy behaviours only have a partial connection.

KEYWORDS

Privacy online, individualism, social influence, Asia, Europe

For More Details: https://aircconline.com/ijsptm/V5N4/5416ijsptm01.pdf

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

REFERENCES

[1] Westin, A. (1967). Privacy and Freedom. New York: Atheneum

[2] Stone, E. F., Gueutal, H., Gardner, D. & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. Journal of Applied Psychology 68, 459-468.

[3] Dhar, S., & Vahrsney, U. (2011). Challenges and business models for mobile location-based services and advertising. Communications of the ACM 54(5), 121-129

[4] Fusco, S. J., Michael, K., & Michael, M. (2010). Using a social informatics framework to study the effects of location-based social networking on relationships between people: A review of literature. IEEE International Symposium on Technology and Society (ISTAS), 157-171.

[5] Beresford, A. R., & Stajano, F. (2003). Location privacy in pervasive computing. IEEE Pervasive Computing 2(1), 46-55.

[6] Webroot (2010), Survey Finds Geolocation Apps Prevalent Amongst Mobile Device Users, But 55% Concerned About Loss of Privacy (www.webroot.com).

[7] Madden, M., & Smith, A. (2010). Reputation management and social media. Pew Internet & American Life Project. Pew Research Center (www.pewinternet.org).

[8] Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly 27, 425-478.

[9] Ajzen, I. (1991). The Theory of Planned Behavior. Organizational Behavior and Human Decision Processes 50, 179-211.

[10] Loch, K. & Conger, S. (1996). Evaluating ethical decision making and computer use. Communications of the ACM 39 (7), 74-83.

[11] Hsu, M. & Kuo, F. (2003). The effect of organization-based self-esteem and deindividuation in protecting personal information privacy. Journal of Business Ethics 42, 305-320.

[12] Zeng, Z., Hu, X. & Mei, S. (2013). Factors affecting a mobile application's acceptance: An empirical study of user acceptance of WeChat in China. Jonkoping International Business School, Jonkoping University.

[13] Xu, H., Teo, H., Tan, B. & Ritu A. (2012). Effects of individual self-protection, industry selfregulation, and government regulation on privacy concerns: A study of location-based services. Information Systems Research 23, 1342-1363.

[14] Notermans, R. (2013). To share or not to share? The personal aspects of online privacy behavior. Tilburg University.

[15] Triandis, H., Bontempo, R., Villareal, M., Asai, M. & Lucca, N. (1988). Individualism and collectivism: Cross-cultural perspectives on self-ingroup relationships. Journal of Personality and Social Psychology 54, 323-338.

[16] Hofstede, G. (2001). Culture's consequences: Comparing values, behaviors, institutions, and organizations across nations. Thousand Oaks, CA: Sage.

[17] McSweeney, B. (2002). Hofstede's model of national cultural differences and their consequences: A triumph of faith - a failure of analysis, Human Relations 55, 89-118.

[18] Hofstede, G. (2002). Dimensions do not exist: A reply to Brendan McSweeney. Human Relations 55, 1355-1361.

[19] Milberg, S., Smith, J. & Burke, S., (2000). Information privacy: Corporate management and national regulation. Organization Science 11, 35-57.

[20] Ting-Toomey, S. (1991). Intimacy expressions in three cultures: France, Japan, and the United States. International Journal of Intercultural Relations 15, 29-46.

[21] Bellman, S., Johnson, E., Kobrin, S., & Lohse, G. (2004). International differences in information privacy concerns: A global survey of consumers. The Information Society 20(5), 313-324.

[22] Lowry, P., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. Journal of Management Information Systems 27(4), 163-200.

[23] Consolvo, S., et al. (2005). Location disclosure to social relations: why, when, & what people want to share. Proceedings of the SIGCHI conference on human factors in computing systems, 81-90.

[24] Wiese, J., et al. (2011). Are you close with me? Are you nearby? Investigating social groups, closeness, and willingness to share. Proceedings of the 13th international conference on ubiquitous computing 197-206.

[25] Kitayama, S., Markus, H., Matsumoto, H. & Norasakkunkit, V. (1997). Individual and collective process in the construction of the self: Self-enhancement in the United States and self-criticism in Japan. Journal of Personality and Social Psychology 72, 1245-1267.

[26] Herrmann-Pillath, C. (2010). Social capital, Chinese style: individualism, relational collectivism and the cultural embeddedness of the institutions-performance link. China Economic Journal 2, 325-350.

[27] Oyserman, D., Coon, H. & Kemmelmeier, M. (2002). Rethinking individualism and collectivism: Evaluation of theoretical assumptions and meta-analyses. Psychological Bulletin 128, 3-72.
[28] Han, M., Yoshiyuki I., Kim, S. & Zhang, W. (2009). The application of culture bounded selfconstrual model: A comparative study between three countries in Northeast Asia. Journal of Korean Psychology Association 28(1), 49-66.
[29] Kwon, J. & Oh, D. (2010). An examination of thirty-year cross-cultural research in Korea: the case of Hofstede's cultural values. International Business Management Review 14 (4), 1-32.
[30] Li, H., Zhang, Z., Bhatt, G., & Yum, Y. (2006). Rethinking culture and self-construal: China as a middle land. The Journal of Social Psychology 146, 591-610.
[31] Buchanan, T., Paine, C., Joinson, A. & Reips, U. (2007). Development of measures of online privacy concern and protection for use on the internet. Journal of the American Society for Information and Science and Technology 58, 157-165.
[32] Chen, R. Wang, J., Heratch, T. & Rao, H. (2011). An investigation of email processing from a risky decision making perspective. Decision Support Systems 52, 73-81.

AUTHORS

Peter Broeder investigates intercultural aspects of online marketing communications and consumer behaviour. These issues are addressed in Europe and Asia (www.broeder.com).

Yujin Lee obtained her master's degree from Tilburg University (the Netherlands) in 2014. Currently she is a Business Development Manager at Research Instruments, Falmouth (United Kingdom).