The International Journal of Network Security & Its Applications (IJNSA)

(ERA, UGC Listed)

Current Issue: November 2018, Volume 10, Number 6 --- Table of Contents

http://airccse.org/journal/jnsa18_current.html

Paper -01

A Multi-Layer Hybrid Text Steganography For Secret Communication Using Word Tagging And RGB Color Coding

Ali F. Al-Azzawi,

Department of Software Engineering, IT Faculty,
Philadelphia University, Amman, Jordan

ABSTRACT

This paper introduces a multi-layer hybrid text steganography approach by utilizing word tagging and recoloring. Existing approaches are planned to be either progressive in getting imperceptibility, or high hiding limit, or robustness. The proposed approach does not use the ordinary sequential inserting process and overcome issues of the current approaches by taking a careful of getting imperceptibility, high hiding limit, and robustness through its hybrid work by using a linguistic technique and a format-based technique. The linguistic technique is used to divide the cover text into embedding layers where each layer consists of a sequence of words that has a single part of speech detected by POS tagger, while the format-based technique is used to recolor the letters of a cover text with a near RGB color coding to embed 12 bits from the secret message in each letter which leads to high hidden capacity and blinds the embedding, moreover, the robustness is accomplished through a multi-layer embedding process, and the generated stego key significantly assists the security of the embedding messages and its size. The experimental results comparison shows that the purpose approach is better than currently developed approaches in providing an ideal balance between imperceptibility, high hiding limit, and robustness criteria.

KEYWORDS

Text Stenography, Python Programming language, Multi-layer encoding, Natural Language Prepossessing, Color space

For More Details: http://aircconline.com/ijnsa/V10N6/10618ijnsa01.pdf
Volume Link: http://airccse.org/journal/jnsa18_current.html

REFERENCES

[1] K. Benett, (2004), “Linguistic Steganography- Survey, Analysis And Robustness Concerns For Hiding Information In Text”, Purdue University, Cerias Tech. Report 2004-13

[2] S Bhattacharya, P Indu, Duta, Sa Biswas, G Sanyal, (2011) “Hiding Data In Text Through In Alphabet Letter Patterns (Calp)”. Journal Of Global Research In Computer Science, 2(3): 33-39

[3] Agarwal, M., (2013). "Text Steganographic Approaches: A Comparison”. Arxiv Preprint Arxiv:1302.2718.

[4] Shirali-Shahreza, M.H. And Shirali-Shahreza, M., (2006), July. “A New Approach To Persian/Arabic Text Steganography”. In Computer And Information Science, 2006 And 2006 1st Ieee/Acis International Workshop On Component-Based Software Engineering, Software Architecture And Reuse. Icis-Comsar 2006. 5th Ieee/Acis International Conference On(Pp. 310-315). Ieee.

[5] S. H. Low, N. F. Maxemchuk, J. T. Brassil, And L. O. Gorman, (1995). “Document Marking And Identification Using Both Line And Word Shifting”, Infocom95 Proceedings Of The Fourteenth Annual Joint Conf. Of The Ieee Computer And Communication Societies, 1995, Pp. 853-860

[6] Singh, H., Singh, P.K. And Saroha, K., (2009), February. “A Survey On Text Based Steganography”. In Proceedings Of The 3rd National Conference (Pp. 26-27).

[7] Taleby Ahvanooey, M., Li, Q., Shim, H.J. And Huang, Y., (2018). “A Comparative Analysis Of Information Hiding Techniques For Copyright Protection Of Text Documents”. Security And Communication Networks, 2018.

[8] Banerjee, I., Bhattacharyya, S. And Sanyal, G., (2011), January. “Novel Text Steganography Through Special Code Generation”. Int. Conf. On Systemics, Cybernetics, And Informatics (Pp. 298-303).

[9] Shirali-Shahreza, M., (2008), February. “Text Steganography By Changing Words Spelling. In Advanced Communication Technology”, Icact 2008. 10th International Conference On (Vol. 3, Pp. 1912-1913). Ieee.

[10] Topkara, M., Topkara, U. And Atallah, M.J., (2006), October. "Words Are Not Enough: Sentence Level Natural Language Watermarking":. In Proceedings Of The 4th Acm International Workshop On Contents Protection And Security (Pp. 37-46). Acm.

[11] Kumar, K.A. And Pabboju, S., (2018). “An Optimized Text Steganography Approach Using Differently Spelt English Words".

[12] Krishnan, R. B., Thandra, P. K., & Baba, M. S. (2017). "An Overview Of Text Steganography. In Signal Processing, Communication And Networking" (Icscn), 2017 Fourth International Conference On (Pp. 1-6). Ieee [13] Jurafsky, D. And Martin, J.H., (2016\4). "Speech And Language Processing". London: Pearson.

[14] Marcus, M.P., Marcinkiewicz, M.A. And Santorini, B., (1993). "Building A Large Annotated Corpus Of English: The Penn Treebank. Computatioal Linguistics", 19(2), Pp.313-330.

[15] Hardeniya, N., Perkins, J., Chopra, D., Joshi, N. And Mathur, I., (2016). "Natural Language Processing: Python And Nltk". Packt Publishing Ltd.

[16] Http://Textx.Readthedocs.Io/En/V1.4.X/#Projects-Using-Textx , Last Visit, September, (2018).

[17] Mokrzycki, W.S. And Tatol, M., 2011. "Colour Difference Δ E-A Survey". Machine Graphics And Vision, 20(4), Pp.383-411.

[18] Patel, I. And Goud, J., (2012). "Colour Recognition For Blind And Colour Blind People". Int J. Eng Innovat Technol, 2(6), Pp.38-42.

[19] Ahvanooey, M.T., Li, Q., Hou, J., Mazraeh, H.D. And Zhang, J., (2018). "Aitsteg: An Innovative Text Steganography Technique For Hidden Transmission Of Text Message Via Social Media". Ieee Access.

[20] Taleby Ahvanooey, M., Dana Mazraeh, H. And Tabasi, S.H., (2016). "An Innovative Technique For Web Text Watermarking" (Aitw). Information Security Journal: A Global Perspective, 25(4-6), Pp.191-196.

[21] Aman, M., Khan, A., Ahmad, B. And Kouser, S., (2017). "A Hybrid Text Steganography Approach Utilizing Unicode Space Characters And Zero-Width Character". International Journal On Information Technologies And Security, 9(1), Pp.85-100.

[22] Alotaibi, R.A. And Elrefaei, L.A., (2018). "Improved Capacity Arabic Text Watermarking Methods Based On Open Word Space". Journal Of King Saud University-Computer And Information Sciences, 30(2), Pp.236-248.

[23] Kouser, S. And Khan, A., (2017). "A Novel Feature Extraction Approach: Capacity Based Zero-Text Steganography". International Journal On Information Technologies And Security, 9(3), Pp.85-98.

[24] Zhang, W., Meng, J. And Ma, C., (2018), June. "Research Progress Of Applying Digital Watermarking Technology For Printing". In 2018 Chinese Control And Decision Conference (Ccdc) (Pp. 4479- 4482). Ieee.

[25] Kamaruddin, N.S., Kamsin, A., Por, L.Y. And Rahman, H., (2018). "A Review Of Text Watermarking: Theory, Methods, And Applications". Ieee Access, 6, Pp.8011-8028.

[26] Kumar, R., Malik, A., Singh, S., Kumar, B. And Chand, S., (2016), April. "A Space Based Reversible High Capacity Text Steganography Scheme Using Font Type And Style". In Computing, Communication, And Automation (Iccca), 2016 International Conference On (Pp. 1090-1094). Ieee.

Paper 02

SECURE THIRD PARTY AUDITOR(TPA) FOR ENSURING DATA INTEGRITY IN FOG COMPUTING

Kashif Munir and Lawan A. Mohammed

University of Hafr Al Batin, KSA

ABSTRACT

Fog computing is an extended version of Cloud computing. It minimizes the latency by incorporating Fog servers as intermediates between Cloud Server and users. It also provides services similar to Cloud like Storage, Computation and resources utilization and security.Fog systems are capable of processing large amounts of data locally, operate on-premise, are fully portable, and can be installed on the heterogeneous hardware. These features make the Fog platform highly suitable for time and location-sensitive applications. For example, the Internet of Things (IoT) devices isrequired to quickly process a large amount of data. The Significance of enterprise data and increased access rates from low-resource terminal devices demands for reliable and low- cost authentication protocols. Lots of researchers have proposed authentication protocols with varied efficiencies.As a part of our contribution, we propose a protocol to ensure data integrity which is best suited for fog computing environment.

KEYWORDS

Protocol, Authentication,Fog Computing, Security Threats, IoT

For More Details: http://aircconline.com/ijnsa/V10N6/10618ijnsa02.pdf
Volume Link: http://airccse.org/journal/jnsa18_current.html

REFERENCES

[1] K. Munir, Lawan A. Mohammad, (2018). Secure Data Integrity Protocol for Fog Computing Environment, Advancing Consumer-Centric Fog Computing Architectures, Ed.KashifMunir, IGI Global Publishing. In Press.

[2] Data Center Companies (2016). Retrieved November, 9, 2017, from https://www.datacenters.com/directory/companies .

[3] Bonomi, F., Milito, R., Zhu, J., &Addepalli, S.(2012). Fog computing and its role in the internet of things. In Proceedings of the first edition of the MCC workshop on Mobile cloud computing. pp 13-16

[4] Sravan Kumar R, AshutoshSaxena,."Data Integrity Proofs in Cloud Storage" 978-1-4244-8953-4/11/$26.00 c 2011 IEEE.

[5] Cisco (2015). Cisco delivers vision of fog computing to accelerate value from billions of connected devices. Retrieved December 02, 2017, from https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1334100

[6] OpenFog Consortium (2015).Retrieved December 02, 2017, from https://www.openfogconsortium.org

[7] Ateniese G., et al.(2007), "Provable data possession at untrusted stores," in Proceedings of CCS'07, New York, USA, pp. 598- 603.

[8] WenjunLuo; GuojingBai "Ensuring the data integrity in cloud data storage" Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference

[9] S. Yi, C. Li, and Q. Li, "A Survey of Fog Computing: Concepts, Applications and Issues," Proc. 2015 Work. Mob. Big Data - Mobidata '15, pp. 37–42, 2015.

[10] Chiang, M., Zhang, T.(2016). Fog and IoT: An overview of research opportunities, IEEE Internet of Things Journal, pp. 1–11.

[11] Bader, A., Ghazzai, H., Kadri, A., &Alouini, M.-S. (2016). Front-end intelligence for large-scale application-oriented Internet-of-things. IEEE Access, vol. 4, pp. 3257–3272, June 2016.

[12] Gentry, C. (2009). Fully homomorphic encryption using ideal lattices In: STOC, vol. 9, 169–178.. ACM.

[13] Bos, JW.,Castryck, W., Iliashenko, I., &Vercauteren, F. (2017). Privacy-friendly forecasting for the smart grid using homomorphic encryption and the group method of data handling. International Conference on Cryptology in Africa, 184–201.. Springer.

[14] Lu, R., Liang, X., Li, X., Lin, X., &Shen, X. (2012).Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. IEEE Trans Parallel Distributed Syst 23(9): 1621–1631

[15] TechTarget (2015), Confidentiality, integrity, and availability (CIA triad), Retrieved April 02, 2018, from: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

[16] Azure (2018), Data Security and Encryption Best Practices, Retrieved April 17, 2018, from https://docs.microsoft.com/en-us/azure/security/azure-security-data-encryption-best-practices

[17] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, (2007), "Provable data possession at untrusted stores," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 598–609.

A.Juels and J. Burton S. Kaliski, (2007), "Pors: Proofs of retrievability for large files," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 584–597.

[18] Polk, T.; McKay, K.; Chokhani, S. (2005).,Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; NIST Special Publication 800-52 Revision 1; NIST: Gaithersburg, MD, USA, 2005.

[19] H. Shacham and B. Waters, (2013), "Compact proofs of retrievability," Journal of Cryptology, vol. 26, pp. 442-483, 2013.

[20] W. Cong, W. Qian, R. Kui, and L. Wenjing, (2010)., "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in INFOCOM,2010 Proceedings IEEE, pp. 1-9.

[21] M. T. Dong and X. Zhou, "Fog Computing: Comprehensive Approach for Security Data Theft Attack Using Elliptic Curve Cryptography and Decoy Technology," OALib, vol. 3, pp. 1–14, 2016

[22] R. Sinha, H. K. Srivastava, and S. Gupta, "Performance Based Comparison Study of RSA," International Journal of Scientific & Engineering Research, vol. 4, no. 4, May 2013.

[23] Lee , K., Kim, D., Ha, D., Rajput, U., & Oh, H. (2015). On security and privacy issues of fog computing supported Internet of Things environment. doi:10.1109/NOF.2015.7333287

[24] N. Mishra, S. Siddiqui, and J. P. Tripathi, "A Compendium Over Cloud Computing Cryptographic Algorithms and Security Issues," Int. J. Inf. Technol. BharatiVidyapeeth's Inst. Comput. Appl. Manag., vol. 7, no. 1, pp. 973–5658, 2015.

[25] L. M. Vaquero, L. R. Merino, (2014), "Finding your Way in the Fog: Towards a Comprehensive Definition of Fog Computing", ACM SIGCOMM Computer Communication Review, vol. 44, no. 5, pp. 27-32, 2014.

[26] T. K. Goyal, V.Sahula. (2016). Lightweight security algorithm for low power IoT devices. International Conference on Advances in Computing, Communications and Informatics (ICACCI).

[27] D. H. Gawali, V. M. Wadhai (2012)., "RC5 Algorithm: potential cipher solution for security in WBSN" International Journal of Advanced Smart Sensor Network System s (IJASSN), Volume 2, No.3, July 2012.

[28] A.Juels and J. Burton S. Kaliski, (2007), "Pors: Proofs of retrievability for large files," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 584–597.

Paper 03

IOT AND SECURITY-PRIVACY CONCERNS: A SYSTEMATIC MAPPING STUDY

Moussa WITTI and Dimitri KONSTANTAS

Information Science Institute University of Geneva
Route de Drize 7, 1227 Carouge, Switzerland

ABSTRACT

The increase of smart devices has accelerated sensitive data exchange on the Internet using most of the time unsecured channels. Since a massive use of RFID (Radio-frequency Identification) tags in the transportation and construction industries from 1980 to 1990, with the expanded use of the Internet with 2G/3G or 4G since 2000, we are witnessing a new era of connected objects. A huge number of heterogeneous sensors may collect and dispatch sensitive data from an endpoint to worldwide network on the Internet. Privacy concerns in IOT remain important issues in the research. In this paper, we aim to evaluate current research state related to privacy and security in IOT by identifying existing approaches and publications trends. Therefore, we have conducted a systematic mapping study using automated searches from selected relevant academics databases. The result of this mapping highlights research type and contribution in different facets and research activities trends in the topic of "security and privacy" in IoT edge, cloud and fog environment.

KEYWORDS

Internet of Thing, privacy, security, the mapping study

For More Details: **http://aircconline.com/ijnsa/V10N6/10618ijnsa03.pdf**
Volume Link: **http://airccse.org/journal/jnsa18_current.html**

REFERENCES

[1] Aaditya Jain, B. S. (2016, April). Internet of Things: Architecture, security goals, and challenges. International Journal Innovative Research in Science & Engineering (IJIRSE), Vol.No2:Issue4.

[2] Alfaqih, T. M., & Al-Muhtadi, J. (2016). Internet of Things Security based on Devices Architecture. International Journal of Computer Applications.

[3] Athreya, A. P., DeBruhl, B., & Tague, P. (2013). Designing for self-configuration and selfadaptation in the “internet of things" in Collaborative Computing: Networking Applications and Worksharing. 9th International Conference Collaboratecom, (pp. 585-592).

[4] Bagozzi, R. Y. (1991). Assessing Construct Validity in Organizational Research. Administrative Science Quarterly (36:3), pp 421-458.

[5] Bouij-Pasquier Imane, A. A. (2015). A Security Framework for Internet of Things. 14 th International conference, CANS 2015, , (pp. 19-31 Volume 9476 of the series Lecture Notes in Computer Science). Marrakesh.

[6] Burnett L., K. B.-S. (Volume 10, Issue 4, May 2003). The GeneTrustee: a universal identification system that ensures privacy and confidentiality for human genetic databases. Journal of law and medicine, 506-513.

[7] Cavalcante E. et al. (2016). On the interplay of Internet of Things and Cloud Computing: A systematic mapping study. Computer Communications Volumes 89-90, Pages 17-33.

[8] Charu C. Aggarwal; Philip S. Yu, eds. (2008). "A General Survey of Privacy". Privacy-Preserving Data Mining – Models and Algorithms

[9] Ding Chao, L. Y. (2011). Security Architecture and Key Technologies for IoT/CPS. ZTE Communication, 17(1):11-16.

[10] Erez Shmueli, T. Z. (2014). Constrained obfuscation of relational databases. Information Sciences,Volume 286, 35.

[11] Gang G., L. Z. (2011). "Internet of things security analysis," in Internet Technology and Applications (iTAP), 2011 International Conference on, 1-4.

[12] Gregor, S. (2006). The Nature of Theory in Information Systems. MIS Quarterly (30:3), 611-642.

[13] Hernandez-Ramos JosAľ L., J. B. (2015). Preserving Smart Objects Privacy through Anonymous. Sensors - Open Access Journal.

[14] Hevner, A. M. (2004). Design Science in Information Systems Research. MIS Quarterly (28:1), 75- 105.

[15] JianQiang Li, J.-J. Y. (2013). A top-down approach for approximate data anonymisation. Enterprise Information Systems, 272.

[16] Junqing Le, X. L. (2016). Full Autonomy: A Novel Individualized Anonymity Model for Privacy Preserving. Computers & Security.

[17] Kocher, P. L. (2004). Security as a new dimension in embedded. In: Proceedings of the 41st Annual Design Automation Conference, DAC 2004, San Diego, CA, USA, June 7-11 (pp. 753-760). New York: ACM.

[18] Liu C., Y. Z. (2012). Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology, in Eighth International Conference on Natural Computation (ICNC).

[19] Leusse P, P. P. (2009). Security Cell, a security model for the Internet of Things and Services. International Conference on in Advances in Future Internet, (pp. 47-52).

[20] Loukil F., Ghedira C., Aïcha-Nabila B., Boukadi K., Maamar Z. Privacy-Aware in the IoT Applications: A Systematic Literature Review. International Conference on Cooperative Information Systems (CoopIS) 2017. Proceedings, Part I. Lecture Notes in Computer Science 10573, Springer 2017, ISBN 978-3-319-69461-0, Oct 2017, Rhodes, Greece.

[21] Mingqiang Xue, P. P. (2011). Distributed privacy preserving data collection. In Proceedings of the 16th international conference on Database systems for advanced applications.

[22] Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian "t-Closeness: Privacy Beyond kAnonymity and l-Diversity," 2007 IEEE 23rd International Conference on Data Engineering, Istanbul, 2007, pp. 106-115.

[23] Pan Yang, X. G. (2013). A Privacy-Preserving Data Obfuscation Scheme Used in Data Statistics and Data Mining. IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing, (p. 881).

[24] Pierangela Samarati and L. Sweeney. k-anonymity: a model for protecting privacy. Proceedings of the IEEE Symposium on Research in Security and Privacy (S&P). May 1998, Oakland, CA.

[25] Kai Petersen, Robert Feldt, Shahid Mujtaba, and Michael Mattsson. 2008. Systematic mapping studies in software engineering. In Proceedings of the 12th international conference on Evaluation and Assessment in Software Engineering (EASE'08), Giuseppe Visaggio, Maria Teresa Baldassarre, Steve Linkman, and Mark Turner (Eds.). BCS Learning & Development Ltd., Swindon, UK, 68-77.

[26] Philipp Offermann, O. L. (2009). Outline of a design science research process. In Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology (DESRIST '09).

[27] Ricardo Neisse, G. S. (2015). A Model-based Security Toolkit for the Internet of Things. ScienceDirect.

[28] Robert Bredereck, A. N. (2014). The effect of homogeneity on the computational complexity of combinatorial data anonymization. Data Mining and Knowledge Discovery, Volume 28, Number 1, 65.

[29] Samani A., H. H. (2015). Privacy in Internet of Things: A Model and Protection Framework. The 6th International Conference on Ambient Systems, Networks and Technologies (ANT-2015), the 5th International Conference on Sustainable Energy Information Technology (SEIT-2015) (pp. Volume 52, 2015, Pages 606-613). Procedia Computer Science.

[30] Shmatikov, J. B. (2006). Efficient anonymity-preserving data collection. In Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD '06). ACM, New York, NY, USA, (pp. 76-85).

[31] Syazarin, N., Aziz, N. A., Daud, S. M., & Syarif, S. A. (2017). An Overview on Security Features or Internet of Things (IoT) in Perception Layer. Journal of Engineering and Applied Sciences.

[32] Usha P., R. S. (2014). Sensitive attribute based non-homogeneous anonymization for privacy preserving data mining. International Conference on Information Communication and Embedded Systems (ICICES2014), 1.

[33] Venable, J. (2006). The Role of Theory and Theorising in Design Science Research. First International Conference on Design Science Research in Information Systems and Technology, (pp. 1-18). Claremont, CA: Claremont Graduate University.

[34] Xiao L, H. B. (2010). A knowledgeable security model for distributed health information systems. Computers & Security., (pp. 331-349).

[35] Xin Ma, Q. H. (2010). Study on the Applications of Internet of Things in the Field of Public Safety. China Safety Science Journal, 20(007):170-176.

[36] Yunjung Lee, Y. P. (2015). "Security Threats Analysis and Considerations for Internet of Things". 2015 8th International Conference on Security Technology (SecTech), (pp. vol. 00, no. , pp. 28- 30).

[37] ZhangW., B. Q. (2013). Security Architecture of the Internet of Things Oriented to Perceptual Layer. in International Journal on Computer, Consumer and Control (IJ3C), Volume 2, No.2.

[38] Zhiqiang Yang, S. Z. (2005). Anonymity-preserving data collection. In Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining (KDD '05). ACM, New York, NY, USA, (pp. 334-343).

Paper 04

BIOMETRIC SMARTCARD AUTHENTICATION FOR FOG COMPUTING

Kashif Munir and Lawan A. Mohammed

University of Hafr Al Batin, KSA

ABSTRACT:

In the IoT scenario, things at the edge can create significantly large amounts of data. Fog Computing has recently emerged as the paradigm to address the needs of edge computing in the Internet of Things (IoT) and Industrial Internet of Things (IIoT) applications. In a Fog Computing environment, much of the processing would take place closer to the edge in a router device, rather than having to be transmitted to the Fog. Authentication is an important issue for the security of fog computing since services are offered to massive-scale end users by front fog nodes.Fog computing faces new security and privacy challenges besides those inherited from cloud computing. Authentication helps to ensure and confirms a user's identity. The existing traditional password authentication does not provide enough security for the data and there have been instances when the password-based authentication has been manipulated to gain access into the data. Since the conventional methods such as passwords do not serve the purpose of data security, research worksare focused on biometric user authentication in fog computing environment. In this paper, we present biometric smartcard authentication to protect the fog computing environment.

KEYWORDS:

Biometric Authentication, Fog Computing, Security

For More Details: http://aircconline.com/ijnsa/V10N6/10618ijnsa04.pdf
Volume Link: http://airccse.org/journal/jnsa18_current.html

REFERENCES

[1] Alrawais, A., Alhothaily, A., Hu, C., & Chang, X. (2017). Fog Computing for the Internet of Things: Security and Privacy Issues. IEEE Internet Computing, vol. 21, no. , pp. 34-42

[2] Balfanz, D., Smetters, D.K., Stewart, P., & Wong, H.C. (2002). Talking to strangers: authentication in ad-hoc wireless networks. Network and Distributed System Security Symposium (NDSS). San Diego, CA USA.

[3] Bonomi, F., Milito, R., Zhu, J., &Addepalli, S.(2012). Fog computing and its role in the internet of things. In Proceedings of the first edition of the MCC workshop on Mobile cloud computing. pp 13- 16

[4] Maher, A.(2015). IoT, from Cloud to Fog Computing (Cisco Blogs). Retrieved November 02, 2018, fromhttps://blogs.cisco.com/perspectives/iot-from-cloud-to-fog-computing Calandriello, G., Papadimitratos, P., Hubaux, J-P., &Lioy, A. (2007). , Efficient and robust pseudonymous authentication in VANET, in: Proc. VANET, pp. 19–28.

[5] Chang, C.,& Tsai, H.-C (2010). An anonymous and self-verified mobile authentication with authenticated key agreement for large-scale wireless networks, IEEE Trans. Wireless Communication. 9 (11) pp. 3346–3353.

[6] Cisco the network in review (2015). Retrieved September 02, 2017, from http://newsroom.cisco.com/featurecontent?type=webcontent&articleId=1365576

[7] Damiani, E., Vimercati, D.C., Paraboshi, S., Samarati, P., &Violante, F. (2002). A reputation-based approach for choosing reliable resources in peer-to-peer networks. Proc. of the 9th ACM conference on Computer and communications security, pp. 207-216.

[8] Deane, F.,Barrelle, K., Henderson, R., & Mahar, D. (2005). Perceived acceptability of biometric security systems. Computers & Security, Vol. 14, N. 3, pp. 225-231.

[9] Dsouza, C., Ahn, G.J., &Taguinod, M. (2014). Policy-driven security management for fog computing: preliminary framework and a case study". Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI).

[10] Gemalto (2018). Biometrics: authentication and identification (2018)- A case study. Retrieve 07 September, 2018, from https://www.gemalto.com/govt/inspired/biometrics

[11] He, D., Ma, M., Zhang, Y., Chen, C., & Bu, J. (2011). A strong user authentication scheme with smart cards for wireless communications, Computer Communications. 34 (3) 367–374.

[12] Josang, A., Ismail, R., & Boyd, C.(2007). A survey of trust and reputation systems for online service provision. Decis. Support Syst. 43(2), 618–644.

[13] Lu, R., Lin, X., Liang, X., & Shen, X. (2010). FLIP: An efficient privacy-preserving protocol for finding like-minded vehicles on the road, in: Proc. IEEE Globecom, pp. 1–5.

[14] Luca, B., Bistarelli, S. &Vaccarelli, A. (2002). Biometrics authentication with smartcard. IIT TR08/2002, Retrieved October, 9, 2017, from http://www.iat.cnr.it/attivita/progetti/parametribiomedici.html

[15] Modi, C., Patel, D., Patel, H., Borisaniya, B., Patel, A. & Rajarajan, M. (2013). A survey of intrusion detection techniques in Cloud. Journal of Network and Computer Applications, 36(1), pp. 42-57

[16] Renu Bhatia (2013), Biometrics and Face Recognition Techniques, International Journal of Advanced Research in Computer Science and Software Engineering Vol. 3, Issue 5, pp 93-99

[17] Sean W. S. & Vernon A. (1998). Trusting Trusted Hardware: Towards a Formal Model for Programmable Secure Coprocessors. Proceedings of the 3rd USENIX Workshop on Electronic Commerce. Boston, Massachusetts, USA.

[18] Shanhe, Yi,.Zhengrui, Q., &Qun, Li. (2015). Security and Privacy Issues of Fog Computing: A Survey. Proc. Int'l Conf. Wireless Algorithms Systems and Applications (WASA) 2015, LNCS 9204, pp. 685–695.

[19] Shi, Y., Abhilash, S., & Hwang, K.(2015). Cloudlet mesh for securing mobile fogs from intrusions and network attacks. In: 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering. pp. 1096-118

[20] Stojmenovic, I., & Wen, S.(2014). The fog computing paradigm: scenarios and security issues. In: Proc. of the 2014 Federated Conference on Computer Science and Information Systems (FedCSIS) conference. pp. 1-8.

[21] Tsai, H., Chang, C., & Chan, K. (2009). Roaming across wireless local area networks using SIM-based authentication protocol, Computer Standard Interfaces 31 (2) pp.381–389.

[22] Tsai, Y. & Chang, C. (2006) , SIM-based subscriber authentication mechanism for wireless local area networks, Computer Communications. 29 (10) pp. 1744–1753.

[23] Vaquero, L.M., &Rodero-Merino, L. (2014). Finding your way in the fog: towards a comprehensive definition of fog computing. ACM SIGCOMM CCR44(5), 27–32

[24] Zhu, H., Lin, X., Lu, R., Ho, P., & Shen, X. (2008). AEMA: An aggregated emergency message authentication scheme for enhancing the security of vehicular Ad Hoc networks, in: Proc. IEEE ICC, pp. 1436–1440.

[25] Calandriello, G., Papadimitratos, P., Hubaux, J-P., &Lioy, A. (2007). , Efficient and robust pseudonymous authentication in VANET, in: Proc. VANET, pp. 19–28.

[26] How to Geek (2014). What is Fog Computing? Retrieved September 02, 2017, From https://www.howtogeek.com/185876/what-is-fog-computing/