Analysis of Cyber Forensics Issues in Internet of Things (IoT)

Mohammad Meraj

March 17, 2022

Analysis of Cyber Forensics Issues in Internet of Things (IoT)

Mohammad Meraj
Department of Computer Science, NIMS University, Jaipur, Rajasthan, India

Abstract: Non-traditional computer devices, such as mechanical and Internet of Things (IoT) devices, may communicate data across a network without human or machine involvement. Because of the Internet of Things, people can live and work more intelligently and with greater freedom. This has also increased the risk of being compromised such as privacy, breach, data breach and integrity issue. Since, the IoT devices are ad-hoc in nature therefore once the crime has taken place then it become a difficult task for the forensic analyst to find the conclusion of the incident. This paper investigates and present the importance of the cyber forensics in IoT.

Keywords: cyber forensics, IoT, device security

1. INTRODUCTION

Continuous hardware miniaturization and increased energy efficiency make it possible to integrate intelligence into ordinary devices. This trend of increasing so-called non-smart everyday devices with computational capabilities has given rise to the Internet of Things (IoT) field. Attackers can infiltrate and exploit IoT systems. Before the advent of the Internet of Things, specialized digital forensic mechanisms were developed to investigate Botnet activities in small systems. As the robotic networks that support IoT are scalable and technically diverse and take advantage of current high-speed networks, developing forensic mechanisms capable of investigating IoT Botnet activities has become an important challenge in the cybersecurity field [1,2,3].

IoT devices are non-traditional computing devices that have the ability to transmit data over a network without the need for human or machine intervention, both mechanical and digital devices The Internet of Things allows individuals to live and work more intelligently and to take complete control of their lives[4,5].

Internet of things devices have become common in our societies, for example in smart cities, smart homes, health care, security, surveillance, inventory management and products, and they are also a source of evidence in criminal investigations, as they generate effects that can be useful for investigation and forensic purposes in any kind of crimes.

One of the challenges facing a digital forensic investigation is the lack of information and the exchange of knowledge between investigators, for example in the investigation process, two or more investigators located in different cities may examine the same device at the same time, and due to the different experiences of each investigator, the results of medical investigations may differ Forensic[5-8].

In addition, due to the sensitive nature of the data obtained from a forensic examination, data is rarely shared.

These challenges may have an impact on the efficiency and timeliness of investigations and results.

This research provides a platform for knowledge sharing using the Internet of Things for forensic practitioners and forensic investigators, as it is difficult for many investigators to work with traditional methods [9-15].

Because every investigator must start from scratch, according to his investigations.

This platform allows investigators to share investigation information so that time is not wasted in starting from the beginning of the investigation [16,17].

As a very rising and revolutionary technology, the internet of Things (IoT) has brought tremendous changes to end-users in their daily lives. Study and work all concerned within the internet of Things, taking advantage of sensible environments (home and city), e-health, transportation systems and anyplace[18-25]. Cybersecurity is that the inevitable drawback that has to be solved within the development of the net of Things. If the matter isn't managed well, hackers can make the most of defects and weaknesses of hardware, objects, or software system then information or systems are discontinuous through the worldwide web of Things. Therefore, forensics analyses necessary to avoid the inevitable issues of a cyberattack, it's essential that user can use the internet of Things without worrying.

One of the writers who talked about the Internet of things is Yang Lu was born in China on First of May, 1979. He received the M.Sc. and Ph.D. degrees from Tianjin University, Tianjin, China, in 2004 and 2007, severally. His Ph.D. supervisor was Jianquan Yao United Nations agency is associate degree Academician of the Chinese Academy of Sciences, Beijing, China. He was associate degree Optical Network Engineer with Tianjin Company Ltd., China Mobile cluster, Tianjin, from 2007 to 2008. He has been with McMaster University, Hamilton, ON, Canada, as a Post-Doctoral Fellow, since 2009. He has intensive expertise in advanced solid-state optical maser and nonlinear optical frequency conversion by exploitation sporadically poled metallic element niobate (PPLN) chips. He was the first Principal of Study on THz radiation exploitation quasi-phase-matched distinction frequency generation tense by all-solid-state dual-wavelength lasers by exploitation PPLN chips supported by the National Science Foundation of China (10474071).,Dr. metallic element was a member of the Ministry of Education Science and Technology cooperated foundation of Nankai University and Tianjin University study on application of recent devices in immoderate broadband fiber communication systems supported nonlinear optical effects

What will be written in this essay is Yang Lu's writing on Internet of Things (IoT) Cybersecurity: here will monition some point from his research: -

The Internet of Things integrates heterogeneous smart devices into an integration network. That is why Cybersecurity of the Internet of Things is a strategy mechanism Improvement, and includes all changes involved In the Internet of Things, to ensure the integrity of the entire all changes concerned common cybersecurity engineering for the Internet of Things from various viewpoints are listed. The cybersecurity frameworks of the Internet of Things fall into three broad categories: a three-layer infrastructure, a four-layer derived architecture, and a five-layer detailed architecture Layers are perception layer (sensor) layer, access layer, layer Network layer, middleware layer, application (service) Layer and interface layer [26-30].

2. APPLICATION OF IOT

In the automotive field, the monitoring system transmits and displays the location and diagnostic data through the cloud provider, which improves the driving experience and helps determine the optimum time for mechanical services [31-35].

In healthcare, the integration of IoT devices has been shown to benefit patients, as vital information can be collected from their homes, contributing to the rapid detection of any deterioration in their condition.

Network Forensics: Evidence is usually short-lived, as packets are produced from a single machine and sent through intermediate nodes to their destination [36].

2.1 IOT MODELS

Device-to-device communication: This type of connection is mainly found in home automation using the Internet of Things [37-38].

Device-to-cloud model: This type of model allows the end user to access their devices through a web interface or smartphone app and view reports from a dataset or change the device's state.

Device-to-cloud model: It is a backend data sharing model, which is a replica of the device model to the cloud, with the added bonus that the user can extract data from the original cloud provider and transfer it to other cloud service providers[39].

Device-to-gateway model: The device communicates with the cloud service provider through the application layer gateway service, which operates on a local machine acting as a proxy .

2.2 DEEP LEARNING AND ITS ROLE IN NETWORK FORENSICS

Artificial Neural Networks (ANNs): are a type of machine learning technology that transforms input data into output through the use of nonlinear transformations. ANNs can be grouped roughly by the number of layers that make up their structure (excluding the input layer), into shallow and deep scripts [40].

Discriminatory models are supervised methods tasked with separating data into classes by focusing on the boundaries of class decision and calculating the conditional probability of a layer feature. Notable examples include [41]:

Recurrent Neural Network (RNN) - can be useful when the information maintains some temporal relationships with its previous states.

Convolutional neural networks (CNNs) - a type of unchanged, multi-layered perception in space, inspired by the interconnections found in the visual cortex of the brain [42].

Challenges inherent in automated internet forensic investigations

Interoperability - Lack of specification clearly causes problems in developing a single forensic solution capable of handling a range of IoT systems and devices

Availability - Services that support IoT may show decreased performance or become completely unavailable.

Cloud storage of information - presents a new set of challenges to forensic investigations, including jurisdiction limitations and conflicting laws as two notable examples.

2.2.1 TRUST-BASED MECHANISM

According to the behavior of nodes in the data forwarding process, a penalty factor is introduced to evaluate the direct trust relationship between nodes and the direct trust value. Then indirect trust value is assigned weights through entropy thus the comprehensive trust value of the evaluated node is obtained. The uncertain set theory is used to classify the trust relationship between nodes, and neighbor nodes with higher trust levels are selected for routing nodes to forward data, and neighbor nodes with lower trust levels will be isolated from the network[42-50]. In addition, in order to prevent normal nodes from being isolated from the network as they are considered as malicious nodes due to some non-intrusive factors, a given recovery time is provided for such nodes to further determine whether or not to isolate them from the network. One of the biggest challenges to overcome this issue is the development of trust mechanism to ensure data exchanges with a certain level of credibility[51-60]. This study proposes a model for trust in IoT networks based on concepts of social networks and criteria of biomedical relevance. The proposed model is based on a recommendation index calculated by a deterministic trust management protocol. To evaluate its effectiveness, simulations were created with different scenarios of IoT networks. The model proved to be useful for detecting objects with suspicious behavior on the network, avoiding the establishment of relationships with these objects and minimizing the damage caused to the IoT during data exchanges. Since its formation, the internet has undergone several transformations among these, one in particular has been drawing attention to the Internet of Things (IoT), which is nothing more than diverse objects connected to the internet and providing services to users, among these objects such as household appliances, wearable, means of transportation, etc[61-65]. The notion is to increasingly connect the physical with the digital world to ensure the security of these devices and for the users themselves. Therefore, it is necessary that the security mechanisms meet the characteristics of the IoT[66-72] .

2.2.2 THE E-R TRUST MODEL

Our experience in cybersecurity has been digitized to offer real-time, autonomous, efficient, scalable, and accurate evaluation flows. Algorithm makes it possible for cognitive systems to continuously mine data and knowledge through advanced analytics. Thus, the focus is to continuously refine methods and processes, so systems should have the ability to identify forensic threats and generate proactive responses. Our collective experience in cybersecurity is encoded in our products. It enables us to process and analyze vast volumes of data and detects impossible threats to humans. Our behavioral biometrics provides an effective way to improve the security posture without disrupting users' experiences and without any hardware requirements. In a world where compliance requirements, reputation protection, UX-based differentiation and cost reduction are top priorities for the vast majority of businesses, behavioral biometric solutions are gaining traction. Institutions and industry leaders have mentioned them as an effective way to move users into the modern authentication flow, which reduces frictions. Different industries are facing the same need: strongly identifying users and preventing fraud, economically and without any complexity.

Honeypot development: Expand the range of IoT simulators and handle massive amounts of inbound traffic.

Network flow analysis: Without fear of privacy violation, it requires less space for saved data compared to other solutions.

Provision of criminal safety: It should be taken in order, to consider how new technologies can be improved to achieve acceptable forensic outcomes.

Dealing with diversity: the speed and volume of IoT data - the large amount and speed with which information is recorded and transmitted.

3. CONCLUSIONS

A new definition of the Internet of Things puts the interconnectivity between "things" and their service-like functions at the fore. Several challenges were presented, including regional jurisdiction issues derived from cloud computing, and some of these trends were: developing and improving honeypots, analysing network flow, and dealing with the vast amounts of high-speed and heterogeneous data produced by the Internet of Things.

Future directions for research have been explored in the field. Some of these directions were: Honeypots and Network Flow analysis creation and enhancement, managing vast amounts of IoT-generated high-speed and heterogeneous data, and proving that any solutions produced are forensically sound and that the results produced will be admissible in a court of law.

Conflict of Interest: There is no conflict of interest and no funding was provided,

REFERENCES

[1] M. A. Khan, "An IoT Framework for Heart Disease Prediction Based on MDCNN Classifier," in IEEE Access, vol. 8, pp. 34717-34727, 2020, doi: 10.1109/ACCESS.2020.2974687.

[2] Khan, M. A, Abuhasel, KA. Advanced metameric dimension framework for heterogeneous industrial Internet of things. Computational Intelligence. 2021; 37: 1367– 1387. https://doi.org/10.1111/coin.12378

[3] Khan, M.A., Abuhasel, K.A. An evolutionary multi-hidden Markov model for intelligent threat sensing in industrial internet of things. J Supercomputing 77, 6236–6250 (2021). https://doi.org/10.1007/s11227-020-03513-6

[4] Khan, M.A., Alghamdi, N.S. A neutrosophic WPM-based machine learning model for device trust in industrial internet of things. J Ambient Intell Human Comput (2021). https://doi.org/10.1007/s12652-021-03431-2

[5] N. S. Alghamdi and M. A. Khan, "Energy-efficient and blockchain-enabled model for internet of things (IoT) in smart cities," Computers, Materials & Continua, vol. 66, no.3, pp. 2509–2524, 2021.

[6] Mahmoud Khalifa, Fahad Algarni, Mohammad Ayoub Khan, Azmat Ullah, Khalid Aloufi, A lightweight cryptography (LWC) framework to secure memory heap in Internet of Things, Alexandria Engineering Journal, Volume 60, Issue 1, 2021, Pages 1489-1497, ISSN 1110-0168, https://doi.org/10.1016/j.aej.2020.11.003.

[7] W. U. Khan, X. Li, A. Ihsan, M. A. Khan, V. G. Menon and M. Ahmed, "NOMA-Enabled Optimization Framework for Next-Generation Small-Cell IoV Networks Under Imperfect SIC Decoding," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2021.3091402.

[8] S. Nandy, M. Adhikari, M. A. Khan, V. G. Menon and S. Verma, "An Intrusion Detection Mechanism for Secured IoMT framework based on Swarm-Neural Network," in IEEE Journal of Biomedical and Health Informatics, doi: 10.1109/JBHI.2021.3101686.

[9] A. Munusamy et al., "Edge-Centric Secure Service Provisioning in IoT-Enabled Maritime Transportation Systems," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2021.3102957.

[10] S. Verma, S. Kaur, M. A. Khan and P. S. Sehdev, "Toward Green Communication in 6G-Enabled Massive Internet of Things," in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5408-5415, 1 April1, 2021, doi: 10.1109/JIOT.2020.3038804

[11] L. Xu, X. Zhou, M. A. Khan, X. Li, V. G. Menon and X. Yu, "Communication Quality Prediction for Internet of Vehicle (IoV) Networks: An Elman Approach," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2021.3088862.

[12] A. Munusamy et al., "Service Deployment Strategy for Predictive Analysis of FinTech IoT Applications in Edge Networks," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3078148.

[13] A. Mukherjee, P. Goswami, M. A. Khan, L. Manman, L. Yang and P. Pillai, "Energy-Efficient Resource Allocation Strategy in Massive IoT for Industrial 6G Applications," in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5194-5201, 1 April1, 2021, doi: 10.1109/JIOT.2020.3035608.

[14] Quasim, M.T. Resource Management and Task Scheduling for IoT using Mobile Edge Computing. Wireless Pers Commun (2021). https://doi.org/10.1007/s11277-021-09087-7

[15] M. A. Khan, M. T. Quasim, N. S. Alghamdi and M. Y. Khan, "A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data," in IEEE Access, vol. 8, pp. 52018-52027, 2020. DOI: 10.1109/ACCESS.2020.2980739

[16] M. T. Quasim, M. A. Khan, M. Abdullah, M. Meraj, S. P. Singh and P. Johri, "Internet of Things for Smart Healthcare: A Hardware Perspective," 2019 First International Conference of Intelligent Computing and Engineering (ICOICE), Hadhramout, Yemen, 2019, pp. 1-5. DOI: 10.1109/ICOICE48418.2019.9035175

[17] M. A. Khan, M. T. Quasim, F. Algarni and A. Alharthi, "Internet of Things: On the Opportunities, Applications and Open Challenges in Saudi Arabia," 2019 International Conference on Advances in the Emerging Computing Technologies (AECT), 2020, pp. 1-5, doi: 10.1109/AECT47998.2020.9194213.

[18] Aileni R.M., Suciu G. (2020) IoMT: A Blockchain Perspective. In: Khan M., Quasim M., Algarni F., Alharthi A. (eds) Decentralised Internet of Things. Studies in Big Data, vol 71. Springer, Cham. https://doi.org/10.1007/978-3-030-38677-1_9

[19] Ansari, Abdul Quaiyum, and Mohammad Ayoub Khan. "Fundamentals of industrial informatics and communication technologies." Handbook of Research on Industrial Informatics and Manufacturing Intelligence: Innovations and Solutions. IGI global, 2012. 1-19.

[20] Khan, Mohammad Ayoub, and Abdul Quaiyum Ansari. "Handbook of Research on Industrial Informatics and Manufacturing Intelligence: Innovations and Solutions." (2012).

[21] Alam, T., Khan, M. A., Gharaibeh, N. K., & Gharaibeh, M. K. (2021). Big data for smart cities: a case study of NEOM city, Saudi Arabia. In Smart cities: a data analytics perspective (pp. 215-230). Springer, Cham.

[22] M. A. Khan and A. Q. Ansari, "n-Bit multiple read and write FIFO memory model for network-on-chip," 2011 World Congress on Information and Communication Technologies, 2011, pp. 1322-1327, doi: 10.1109/WICT.2011.6141440.

[23] S. Tyagi, A. Q. Ansari and M. A. Khan, "Dynamic threshold-based sliding-window filtering technique for RFID data," 2010 IEEE 2nd International Advance Computing Conference (IACC), 2010, pp. 115-120, doi: 10.1109/IADCC.2010.5423025.

[24] Khan, Mohammad Ayoub, and Abdul Quaiyum Ansari. "A quadrant-XYZ routing algorithm for 3-D asymmetric torus network-on-chip." The Research Bulletin of Jordan ACM, ISSN (2011): 2078-7952.

[25] M. Ayoub Khan and S. Ojha, "Virtual Route Tracking in ZigBee (IEEE 802.15.4) enabled RFID interrogator mesh network," 2008 International Symposium on Information Technology, 2008, pp. 1-7, doi: 10.1109/ITSIM.2008.4631904.

[26] Khan M.A., Algarni F., Quasim M.T. (2020) Decentralised Internet of Things. In: Khan M., Quasim M., Algarni F., Alharthi A. (eds) Decentralised Internet of Things. Studies in Big Data, vol 71. Springer, Cham. https://doi.org/10.1007/978-3-030-38677-1_1

[27] M. Ayoub Khan and Y. P. Singh, "On the security of joint signature and hybrid encryption," 2005 13th IEEE International Conference on Networks Jointly held with the 2005 IEEE 7th Malaysia International Conf on Communic, 2005, pp. 4 pp.-, doi: 10.1109/ICON.2005.1635449.

[28] Bhardwaj R., Datta D. (2020) Consensus Algorithm. In: Khan M., Quasim M., Algarni F., Alharthi A. (eds) Decentralised Internet of Things. Studies in Big Data, vol 71. Springer, Cham. https://doi.org/10.1007/978-3-030-38677-1_5

[29] Quasim M.T., Khan M.A., Algarni F., Alshahrani M.M. (2021) Fundamentals of Smart Cities. In: Khan M.A., Algarni F., Quasim M.T. (eds) Smart Cities: A Data Analytics Perspective. Lecture Notes in Intelligent Transportation and Infrastructure. Springer, Cham. https://doi.org/10.1007/978-3-030-60922-1_1

[30] Khan, M. A., & Ansari, A. Q. (2011, March). 128-Bit High-Speed FIFO Design for Network-on-Chip,”. In Proc (pp. 116-121).

[31] Khan, M. A., Quasim, M. T., Algarni, F., & Alharthi, A. (Eds.). (2020). Decentralised Internet of Things: A blockchain perspective (Vol. 71). Springer Nature.

[32] Chawki M., Darwish A., Khan M.A., Tyagi S. (2015) 419 Scam: An Evaluation of Cybercrime and Criminal Code in Nigeria. In: Cybercrime, Digital Forensics and Jurisdiction. Studies in Computational Intelligence, vol 593. Springer, Cham. https://doi.org/10.1007/978-3-319-15150-2_9

[33] Khan, Mohammad Yahiya, Sapna Tyagi, and Mohammad Ayoub Khan. "Tree-Based 3-D Topology for Network-on-Chip World." Applied Sciences Journal 30.7 (2014): 844-851.

[34] Ansari, A. Q., & Khan, M. A. (2013). Architecture of 3-D network-on-chip (NoC) router with guided flit logic. filed with Indian Patent office.

[35] Ansari AQ, Ansari MR, Khan MA. Performance evaluation of various parameters of Network-on-Chip (NoC) for different topologies. In2015 annual IEEE India conference (INDICON) 2015 Dec 17 (pp. 1-4). IEEE.

[36] Ansari, A. Q., & Khan, M. A. (2012). A Journey from Computer Networks to Networks-on-Chip. IEEE Beacon, 31(1), 71-77.

[37] Khan, M. A., & Ansari, A. Q. (2011, December). An efficient tree-based topology for Network-on-Chip. In 2011 World Congress on Information and Communication Technologies (pp. 1316-1321). IEEE.

[38] Gandhi, M., & Khan, M. A. (2014, November). Performance analysis of metrics of broadcasting protocols in VANET. In 2014 Innovative Applications of Computational Intelligence on Power, Energy and Controls with their impact on Humanity (CIPECH) (pp. 315-321). IEEE.

[39] Tyagi, S., & Khan, M. A. (2013). Topologies and routing strategies in MPSoC. International Journal of Embedded Systems, 5(1-2), 27-35.

[40] Khan, Mohammad Ayoub, and Abdul Quaiyum Ansari. "Design of 8-bit programmable crossbar switch for network-on-chip router." Trends in Network and Communications (2011): 526-535.

[41] Ansari, Abdul Quaiyum, Mohammad Rashid Ansari, and Mohammad Ayoub Khan. "Performance evaluation of various parameters of Network-on-Chip (NoC) for different topologies." In 2015 annual IEEE India conference (INDICON), pp. 1-4. IEEE, 2015.

[42] Halima, N. B., Khan, M. A., & Kumar, R. (2015, June). A novel approach of digital image watermarking using HDWT-DCT. In 2015 Global Summit on Computer & Information Technology (GSCIT) (pp. 1-6). IEEE.

[43] Mohammad Ayoub Khan, Mohammad Tabrez Quasim , et.al, Decentralised IoT, Decenetralised IoT: A Blockchain perspective, Springer, Studies in BigData, 2020, DOI: https://doi.org/10.1007/978-3-030-38677-1

[44] Quasim M.T., Khan M.A., Algarni F., Alharthy A., Alshmrani G.M.M. (2020) Blockchain Frameworks. In: Khan M., Quasim M., Algarni F., Alharthi A. (eds) Decentralised Internet of Things. Studies in Big Data, vol 71. Springer, DOI: https://doi.org/10.1007/978-3-030-38677-1

[45] M. A. Khan, M. T. Quasim, N. S. Alghamdi and M. Y. Khan, "A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data," in IEEE Access, vol. 8, pp. 52018-52027, 2020. DOI: 10.1109/ACCESS.2020.2980739

[46] M. T. Quasim, M. A. Khan, M. Abdullah, M. Meraj, S. P. Singh and P. Johri, "Internet of Things for Smart Healthcare: A Hardware Perspective," 2019 First International Conference of Intelligent Computing and Engineering (ICOICE), Hadhramout, Yemen, 2019, pp. 1-5. DOI: 10.1109/ICOICE48418.2019.9035175

[47] Sivaram, M., Rathee, G., Rastogi, R. et al. A resilient and secure two-stage ITA and blockchain mechanism in mobile crowd sourcing. J Ambient Intell Human Comput (2020). https://doi.org/10.1007/s12652-020-01800-x

[48]M. T. Quasim, A. A. E. Radwan, G. M. M. Alshmrani and M. Meraj, "A Blockchain Framework for Secure Electronic Health Records in Healthcare Industry," 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), Bengaluru, 2020, pp. 605-609, doi: 10.1109/ICSTCEE49637.2020.9277193.

[49] M. Meraj, S. P. Singh, P. Johri and M. T. Quasim, "An investigation on infectious disease patterns using Internet of Things (IoT)," 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), Bengaluru, 2020, pp. 599-604, doi: 10.1109/ICSTCEE49637.2020.9276922.

[50] M. Tabrez Quasim, F. Algarni, A. Abd Elhamid Radwan and G. M. M. Alshmrani, "A Blockchain based Secured Healthcare Framework," 2020 International Conference on Computational Performance Evaluation (ComPE), Shillong, India, 2020, pp. 386-391, doi: 10.1109/ComPE49325.2020.9200024.

[51] M. A. Khan, M. T. Quasim, F. Algarni and A. Alharthi, "Internet of Things: On the Opportunities, Applications and Open Challenges in Saudi Arabia," 2019 International Conference on Advances in the Emerging Computing Technologies (AECT), Al Madinah Al Munawwarah, Saudi Arabia, 2020, pp. 1-5, doi: 10.1109/AECT47998.2020.9194213.

[52]]Khan, M. A, Algarni F, Quasim M.T,(2021). Smart Cities: A Data Analytics Perspective.

https://doi.org/10.1007/978-3-030-60922-1. . 978-3-030-60921-4

[53] M. Meraj, S. P. Singh, P. Johri and M. T. Quasim, "An investigation on infectious disease patterns using Internet of Things (IoT)," 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), 2020, pp. 599-604, doi: 10.1109/ICSTCEE49637.2020.9276922.

[54] H. Alqarni, W. Alnahari and M. T. Quasim, "Internet of Things (IoT) Security Requirements: Issues Related to Sensors," 2021 National Computing Colleges Conference (NCCC), 2021, pp. 1-6, doi: 10.1109/NCCC49330.2021.9428857.

[55] M. Meraj, S. A. M. Alvi, M. T. Quasim and S. W. Haidar, "A Critical Review of Detection and Prediction of Infectious Disease using IOT Sensors," 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), 2021, pp. 679-684, doi: 10.1109/ICESC51422.2021.9532992.

[56] W. Alnahari and M. T. Quasim, "Privacy Concerns, IoT Devices and Attacks in Smart Cities," 2021 International Congress of Advanced Technology and Engineering (ICOTEN), 2021, pp. 1-5, doi: 10.1109/ICOTEN52080.2021.9493559.

[57] Meraj, M., Singh, S. P., Johri, P., & Quasim, M. T. (2021, April). Detection and Prediction of Infectious Diseases Using IoT Sensors: A Review. In Smart Computing: Proceedings of the 1st International Conference on Smart Machine Intelligence and Real-Time Computing (SmartCom 2020), 26-27 June 2020, Pauri, Garhwal, Uttarakhand, India (p. 56). CRC Press.

[58] W. Alnahari and M. T. Quasim, "Authentication of IoT Device and IoT Server Using Security Key," 2021 International Congress of Advanced Technology and Engineering (ICOTEN), 2021, pp. 1-9, doi: 10.1109/ICOTEN52080.2021.9493492.

[59] Mohammad Tabrez Quasim, et.al 5V'S OF BIG DATA VIA CLOUD COMPUTING: USES AND IMPORTANCE, Sci.int(Lahore),vol.31(3),PP.367-371,2019

[60] Dr. Md. Tabrez Quasim and Mohammad. Meraj, Big Data Security and Privacy: A Short Review, International Journal of Mechanical Engineering and Technology, 8(4), 2017, pp. 408-412. http://www.iaeme.com/IJMET/issues.asp?JType=IJMET&VType=8&IType=4

[61] M.T. Quasim ,et.al . Artificial Intelligence as a Business Forecasting and Error Handling Tool. COMPUSOFT, An international journal of advanced computer technology, 4 (2), February-2015 (Volume-IV, Issue-II).

[62]M.T. Quasim ,Security Issues in Distributed Database System Model , COMPUSOFT, An international journal of advanced computer technology, 2 (12), December-2013 (Volume-II, Issue-XII)

[63] MA Ali, MT Quasim, MA Farah, et .al," CSTNPD: A Database for Cancer Specific Toxic Natural Products" , Indian Journal of Science and Technology, Vol 12(10), DOI: 10.17485/ijst/2019/v12i10/141396, March 20192019,

[64] M.T.Quasim , An Efficient approach for concurrency control in distributed database system, Indian Streams Research Journal, 2013(Volume-3, Issue-9)

[65] S. S. Kshatri, D. Singh, B. Narain, S. Bhatia, M. T. Quasim and G. R. Sinha, "An Empirical Analysis of Machine Learning Algorithms for Crime Prediction Using Stacked Generalization: An Ensemble Approach," in IEEE Access, vol. 9, pp. 67488-67500, 2021, doi: 10.1109/ACCESS.2021.3075140.

[66] MT Quasim, A Shaikh, M Shuaib, A Sulaiman, S Alam, and Y Asiri, "Smart Healthcare Management Evaluation using Fuzzy Decision Making Method,"Apr. 2021, doi: 10.21203/RS.3.RS-424702/V1

[66] Quasim, M. T., Alhuwaimel, S., Shaikh, A., Asiri, Y., Rajab, K. et al. (2021). An Improved Machine Learning Technique with Effective Heart Disease Prediction System. CMC-Computers, Materials & Continua, 69(3), 4169–4181.

[67] Perumal, S., Tabassum, M., Narayana, G., Ponnan, S., Chakraborty, C. et al. (2021). ANN Based Novel Approach to Detect Node Failure in Wireless Sensor Network. CMC-Computers, Materials & Continua, 69(2), 1447–1462.

[68] R. Farkh, H. Marouani, K. A. Jaloud, S. Alhuwaimel, M. T. Quasim et al., "Intelligent autonomous-robot control for medical applications," Computers, Materials & Continua, vol. 68, no.2, pp. 2189–2203, 2021.

[69] R. Farkh, M. T. Quasim, K. Al jaloud, S. Alhuwaimel and S. T. Siddiqui, "Computer vision-control-based cnn-pid for mobile robot," Computers, Materials & Continua, vol. 68, no.1, pp. 1065–1079, 2021.

[70] Meraj, M., Singh, S. P., Johri, P., & Quasim, M. T. (2021). An Analysis of Malaria Prediction through ML-Algorithms in Python and IoT Adoptability. Annals of the Romanian Society for Cell Biology, 25(6), 14098-14107.

[71] Quasim, M.T., Alkhammash, E.H., Khan, M.A. et al. Emotion-based music recommendation and classification using machine learning with IoT Framework. Soft Comput 25, 12249–12260 (2021). https://doi.org/10.1007/s00500-021-05898-9

[72] Ebrahim, N. S., & Quasim, M. T. (2021). EMCSS: efficient multi-channel and time-slot scheduling. Wireless Networks, 27(4), 2879-2890.