Review of Machine Learning Algorithms in Future Smart Cities

Xu Hwanwg

May 17, 2022

Review of Security Issues in smart cities

Xu Hwanwg

Computing Laboratory, Fudan University, China

Abstract: Intelligent transmission systems, like other wireless networks, are subject to numerous security assaults, and adequate countermeasures are necessary to protect the corresponding applications. One of the most important criteria for a secure vehicle network is availability, which guarantees data transmission within latency constraints utilizing low-weight and lightweight encryption methods. Vehicle identification and data are entirely anonymous thanks. These component in smart cities are becoming extremely important and must be addressed.

1 Introduction

The population of the areas is quickly expanding nowadays. Several towns started to build their own smart city policies in order to enhance the quality of life and deliver better services to inhabitants [1].

Many nations experiencing population boom are investing heavily in smart city initiatives. Smart city technologies, for example, allow life to manage its day-to-day operations in order to make people's lives simpler. Smart city infrastructure consists of numerous linked devices and systems that help people in a range of applications, including smart healthcare, smart transit, smart parking, smart traffic systems, smart agriculture, and smart residences, to mention a few [2,3,4,5].

ICN (information-based networking) is a network paradigm that can sustain packet delivery in unstable situations. As a result, in smart cities, ICN might be viewed as an alternative to IP-based networks [6].

The incorporation of various low-cost smart devices such as sensors and actuators, as well as the rapid development of wireless communication technologies that enable small and low-cost objects to connect to the Internet, have aided the spread of the Internet of Things (IoT), in which physical objects transform into smart things in everyday life[7]. ICN solutions, when combined with IP-based methodologies such as those provided in Shenget al's work, may be used to accelerate the rise of IoT and related applications. Instead of depending on IP host identification, information-centric networks have the benefit of having a notion for designating content and finding information in the architectural center 6. [8]

Cities are becoming smarter, which may expose individuals to significant security and privacy threats owing to the nature of gadgets with limited resources, making the smart city susceptible to numerous security assaults. These flaws might lead to a slew of cyber-attacks. In intelligent cities. Malicious attackers, for example, may generate false data while altering sensor data, resulting in a loss of control over highly intelligent systems [9-15]. A hacking assault caused a massive power outage for 230,000 people in Ukraine in 2015. Many devices with limited resources, such as sensors and cameras, which gather and communicate sensitive data in smart cities, might also be subject to hostile hacker assaults, threatening people's security and privacy [16-20]. As a result of these cyber-attacks, home area information gathered and managed by smart homes may give a means to learn about people's lifestyles. In terms of privacy, cloud computing may offer cost-effective data processing and storage services [21,22]. However, several concerns with cloud-based IoT applications, such as a lack of navigation, location awareness, latency, and security, may be addressed using a fog computing architecture [23]. Fog Computing tackles these issues by offering computing resources to consumers at the network's edge, which reduces latency and improves service quality. However, security and privacy are two significant concerns in fog computing owing to differences in fog computing and cloud computing that make cloud security solutions unsuitable for fog computing services exposed to users[24]. Security assaults may be mitigated using a variety of encryption approaches. These technologies, however, are unsuitable for resource-constrained IoT devices in smart cities. Offloading extra security-related tasks to a fog-based node, which may allow security and data analysis directly at the network's edge, might be one approach in this area [25-30].

The smart city idea, according to IBM, is centered on three basic characteristics:'staged,' 'interconnected,' and'smart'[31-36].

This characteristic refers to a city that is covered by a network of devices such as sensors and actuators. As a result of these devices, city platforms have access to trustworthy and current information [37-45].

Connected: A smart city has a large number of systems that work together to give information from many areas and sources. Then, employing a specific combination of networked and equipped systems, a connection from the physical world to the actual world may be established [46-50].

Smart: refers to a planned and networked environment that utilizes data from numerous systems and devices, such as sensors, to enhance residents' quality of life.

2 Background and Related Work

The complex and linked character of smart cities poses significant political, technological, and socioeconomic issues for the designers, integrators, and organizations in charge of these new entities [51-67]. An rising number of studies concentrate on smart city security, privacy, and dangers, emphasizing threats to information security and the issues that smart city infrastructure faces in handling and processing personal data [68, 69]. This research examines many of these issues and offers a useful synthesis of the relevant primary literature as well as the growth of the smart city interaction framework [70]. The research is organized around a number of key topics in smart city research, including: privacy and security of mobile devices and services [71], smart city infrastructure, energy and healthcare systems, frameworks, algorithms, and protocols to improve security, privacy, operational threats to smart cities, use and adoption of smart services by citizens, use of blockchain, and use of social media [72-80]. This detailed analysis gives a valuable perspective on numerous critical topics and serves as the primary path for future research. The findings of this study may serve as an informative research framework and a point of reference for academics and practitioners.

Concerns about privacy and cyber-attacks in smart cities

Almost every element of personal privacy is likely to be jeopardized in a smart city; sensitive personal information such as location, identity, habits, and social interactions will be infringed if not well safeguarded. In order to provide our readers with a better knowledge of privacy concerns in a smart city setting, we will go through the major difficulties that have been discovered or investigated from the standpoint of numerous smart applications [81-56].

Security threats and countermeasures

Intelligent transmission systems, like other wireless networks, are subject to numerous security assaults, and adequate countermeasures are necessary to protect the corresponding applications. One of the most important criteria for a secure vehicle network is availability, which guarantees data transmission within latency constraints utilizing low-weight and lightweight encryption methods [87]. Vehicle identification and data are entirely anonymous thanks to confidentiality. Another important security aspect is authentication, which guarantees that messages are transmitted by a valid ITS station, that neighboring traffic sites are correctly checked, and that hostile users' data assaults are prohibited. Delegation is a critical security need for determining proper data access control for different ITS terminals [88]. Another security concern is ensuring data integrity and ensuring that data has not been altered by a hostile user.

[89] illustrates a list of security threats, security needs that constitute a danger, and viable responses. DoS attacks have an impact on service availability and, as a result, the quality of service for security applications. Jamming assaults, which broadcast a noise signal over the physical channel to raise interference levels and distort communications, fall under this category. Spam assaults, on the other hand, inject a huge number of bogus messages into the network in order to make the channel busy and inaccessible [90]. Sybil attacks employ bogus node identities to send phony messages, which may create network congestion and distribute incorrect information [91]. Additional assaults on network availability include malware, spam, black holes, gray holes, sink holes, and warm holes [92]. Digital signature techniques may be used to defeat the majority of these assaults.

3 Security Issues in Smart Cities

Privacy protection has become one of the biggest problems in our data-driven society. Many related studies have been completed in the past two decades. Clustering-based methods are first applied in privacy protection domains [95-100]. Differential privacy, due to its rigorous privacy guarantee, has attracted increasing attention and applications. In this section, we focus on the domain of the Smart City, and try to provide an extensive review of developed protection technologies, which are summarized from the perspective of different disciplines [95-96].
Smart metering infrastructure is an important component of smart grids, which enable distributed system operators to record real-time power consumption periodically and optimize services for residents. However, the ability to mon- itor power flows also raises concerns about privacy, because it can expose the private life of residents (e.g., living habits, working hours,

and whether the residents are away from their home) [93]. If the data is stolen by attackers or illegally used by untrusted system operators, the privacy of customers might be compromised. Therefore, how to protect a residence's sensitive information has become a hot research topic [94].

3.1 CONVENTIONAL APPROACHES

Cryptographic algorithms are the most frequently used privacy protection method in the IoT domain. Many cryptographic tools have been applied in practice. Unfortunately, traditional encryption mechanisms with overly computational complexity cannot meet the new requirements for smart applications, especially for those systems that consist of many resource-constraint devices. Consequently, how to develop lightweight yet effective encryption algorithms is of significant practical value.

Homomorphic encryption (HE), as a method of performing calculations on encrypted information, has received increasing attention in recent years. The key function of it is to protect sensitive information from being exposed when performing computations on encrypted data. For example, Abdallah et al. developed a lightweight HE-based privacy protection data aggregation method for smart grids that can avoid involving the smart meter when aggregate readings are performed. Another work by Talpur et al. proposed an IoT network architecture based on HE technology for healthcare monitoring systems. Despite the great potential of HE methods, computational expense may restrict the application of this method.

Zero-knowledge proof is another cryptographic method that allows one party to prove something to other parties, without conveying additional information. For application in the Smart City domain, Dousti et al. developed an authentication protocol for smart cards through zero-knowledge proofs.

3.2 CIPHER METHODS

The Kaiser code is a form of substitution code, however it is one of the simplest since the replacement code may be used to build numerous complicated codes. For example, the table below depicts a basic replacement algorithm based on the key. 123 Plaintext I T P E D I A A I T P E D I A I T P E D I A I +1 +2 +3 +1 +2 +3 +1 +2 +2 Ciphertext B K W Q G G J C B K W Q G G J C B K W Q G G J A more advanced replacement technique, not based on the designation, may be employed against each letter in the alphabet with another letter. For instance, we may use the following key:

The issue is, why did we choose the key (DKVQFIBJWPESCXHTMYAUOLRGZN), and does it follow any rules? This key is generated at random, and there is no special rule for doing so, however we aim to divide the letters as evenly as possible. As an example: If we use this approach to encode ait pedia, it will be in the form Plaintext. AITPEDIA Ciphertext DWUTFQWD Breaking the basic substitution method is more harder than breaking Caesar's algorithm. In Caesar's method, knowing the original letter matching to a blinded letter leads to knowledge of the other letters; however, in the replacement algorithm, the range of values or tries required to break the system is 26 × 25 x 24 x... x 1, which equals 26! It is about equivalent to 4 1026 and is a big field with stronger resistance to penetration. This strategy is insufficient, and the difficulty is that the language (whether Arabic or English) has repetition since the letters are not used in the same order. Attempts to break this system are based on the original language's character frequency, which is estimated by evaluating a huge number of texts. Assuming, for example, that the frequency of the letter e is 13%, we may determine the frequency of the letters in the encrypted language. If we discover that the letter t, for example, has a frequency close to this frequency, the letter t in the blind language is often offset by the letter e in the original language. Take the following text as an example: UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX EPYEPOPDZSZUFPOMBZMJDFUDZ To locate the original text, we compute the most common letter in the text, and for the purpose of speculation, we make P = e, Z = t, and by guesswork, we also create ZW = th, so that it is ZWP = the, and after many tries, we obtain the following text: Yesterday, it was revealed that many casual but direct connections had been established with political figures in Moscow.

4 Conclusion

Cities have evolved into dynamic smart homes as they develop and flourish. Indeed, many governments have initiated smart city programs, which represent the greatest method to make cities smart. In reality, IoT may be used in a variety of contexts, including building health monitoring through passive WSN networks and environmental monitoring. Gas concentration, lake water level, or soil moisture, waste management, smart parking, carbon dioxide emissions reduction, or self-driving vehicles are all examples of examples of examples of examples of examples of examples of examples of examples of examples of examples of examples of examples of examples of Such objectives need a massive number of interconnected items. In reality, the number of linked things is growing rapidly, and it is anticipated that 50 billion connected objects will be deployed in smart cities by 2020; nevertheless, this enormous number will raise numerous hazards and privacy concerns, and we have presented an overview of the Internet in this work. Things in the context of smart cities, and we addressed how they may improve city intelligence, as well as the flaws and hazards linked with the expansion and use of the Internet.

Reference

1. Abuhasel, K. A., & Khan, M. A. (2020). A secure industrial Internet of Things (IIoT) framework for resource management in smart manufacturing. IEEE Access, 8, 117354-117364.
2. 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.
3. Al-Qahtani, Awad Saad, and Mohammad Ayoub Khan. "Predicting Internet of Things (IOT) Security and Privacy Risks–A Proposal Model, Journal of Engineering Sciences and Information Technology, pp. 112-133, 5(3), 2021, https://doi.org/10.26389/AJSRP.Q070621
4. Rashmi Bhardwaj, Varsha Duhoon, Mohammad Ayoub Khan, Smart Technologies and Social Impact: An Indian Perspective of Contactless Technologies for Pandemic,
5. Malik Khlaif Gharaibeh , Natheer Khlaif Gharaibeh, Mohammad Ayoub Khan, Waleed Abdel karim Abu-ain and Musab Kasim Alqudah, Intention to Use Mobile Augmented Reality in the Tourism Sector, Computer Systems Science & Engineering, vol.37, no.2, pp. 187-202, https://www.techscience.com/csse/v37n2/41450/pdf
6. 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.
7. 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.
8. Bhulania, Paurush, M. R Tripathy, and Ayoub Khan. "High-Throughput and Low-Latency Reconfigurable Routing Topology for Fast AI MPSoC Architecture." In Applications of Artificial Intelligence and Machine Learning, pp. 643-653. Springer, Singapore, 2021. https://doi.org/10.1007/978-981-16-3067-5_48
9. Khan, Mohammad Ayoub, Rijwan Khan, Fahad Algarni, Indrajeet Kumar, Akshika Choudhary, and Aditi Srivastava. "Performance evaluation of regression models for COVID-19: A statistical and predictive perspective." Ain Shams Engineering Journal 13, no. 2 (2022): 101574., https://doi.org/10.1016/j.asej.2021.08.016
10. 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.
11. Khan, M. A. (2021). A formal method for privacy-preserving in cognitive smart cities. Expert Systems, e12855. https://doi.org/10.1111/exsy.12855
12. 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.

13. P. Bhulania, M. Ranjan Tripathy and A. Khan, "A routing protocol based on priority based adaptive for MPSoC for data transmission," *2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, 2020, pp. 445-449, doi: 10.1109/ICACCCN51052.2020.9362744.
14. 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
15. 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.
16. Khan, M. A., & Algarni, F. (2020). A healthcare monitoring system for the diagnosis of heart disease in the IoMT cloud environment using MSSO-ANFIS. IEEE Access, 8, 122259-122269.
17. Mohammad Rashid Ansari, Abdul Quaiyum Ansari & Mohammad Ayoub Khan (2017) Design and Evaluation of Binary-Tree Based Scalable 2D and 3D Network-on-Chip Architecture, Smart Science, 5:4, 194-198, DOI: 10.1080/23080477.2017.1383078
18. Y. Yang *et al*., "ASTREAM: Data-Stream-Driven Scalable Anomaly Detection with Accuracy Guarantee in IIoT Environment," in *IEEE Transactions on Network Science and Engineering*, doi: 10.1109/TNSE.2022.3157730.
19. Mohammad Ayoub Khan, Amit Kumar, Scalable Design and Processor Technology for IoT Applications, Khan, M.A. (Ed.). (2022). Internet of Things: A Hardware Development Perspective (1st ed.). CRC Press. https://doi.org/10.1201/9781003122357
20. Algarni, Fahad, and Mohammad Ayoub Khan. "Intelligent Electric Vehicle to Predict the Accident and Notify before Accident." U.S. Patent Application No. 17/245,407.
21. 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
22. 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.
23. 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.
24. 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
25. 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.
26. 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.

27. Khan, M.A., Gairola, S., Jha, B. and Praveen, P. eds., 2021. 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. CRC Press.
28. 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
29. P. Bhulania, M. R. Tripathy and Mohammad Ayoub. Khan, "3D implementation of heterogeneous topologies on MPSoC," *2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence*, 2017, pp. 470-473, doi: 10.1109/CONFLUENCE.2017.7943197.
30. Ansari, Abdul Quaiyum, Mohammad Rashid Ansari, and Mohammad Ayoub Khan. "Modified quadrant-based routing algorithm for 3D Torus Network-on-Chip architecture." Perspectives in science 8 (2016): 718-721.
31. Sharma, Manoj, Ruchi Gautam, and Mohammad Ayoub Khan, eds. Design and Modeling of Low Power VLSI Systems. IGI Global, 2016.
32. Ravulakollu, Kiran Kumar, Mohammad Ayoub Khan, and Ajith Abraham. Trends in ambient intelligent systems. Springer, Cham, 2016.
33. 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.
34. Nadhir Ben Halima and Mohammad Ayoub Khan. 2015. Routing in Cognitive Wireless Mesh Networks. In Proceedings of the 12th International Joint Conference on e-Business and Telecommunications - Volume 1 (ICETE 2015). SCITEPRESS - Science and Technology Publications, Lda, Setubal, PRT, 43–48. https://doi.org/10.5220/0005571000430048
35. N. Ben Halima and M. Ayoub Khan, "Routing in Cognitive Wireless Mesh Networks an intelligent framework," 2015 12th International Joint Conference on e-Business and Telecommunications (ICETE), 2015, pp. 43-48.
36. N. B. Halima, M. A. Khan and R. Kumar, "A novel approach of digital image watermarking using HDWT-DCT," 2015 Global Summit on Computer & Information Technology (GSCIT), 2015, pp. 1-6, doi: 10.1109/GSCIT.2015.7353317.
37. Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi Cybercrime, Digital Forensics and Jurisdiction, Springer 2016, https://doi.org/10.1007/978-3-319-15150-2
38. Ansari, Abdul Quaiyum, Mohammad Ayoub Khan, and Mohammad Rashid Ansari. "Advancement in energy efficient routing algorithms for 3-D Network-on-Chip architecture." Proc. National Conference on Emerging Trends and Electrical and Electronics Engg.(ETEEE-2015), New Delhi. 2015.
39. Tiwari, S.C, Gupta, M., Khan, M.A., Ansari, A.Q., Intellectual property rights in semi-conductor industries: An Indian perspective, Business Strategies and Approaches for Effective Engineering Management, 2013, 10.4018/978-1-4666-6433-3.ch013
40. 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.

41. Kathuria, Jagrit, et al. "Low Power Techniques for Embedded FPGA Processors." Embedded and Real Time System Development: A Software Engineering Perspective. Springer, Berlin, Heidelberg, 2014. 283-304.
42. Mohammad Ayoub Khan, Saqib Saeed, Ashraf Darwish, Ajith Abraham, Embedded and Real Time System Development: A Software Engineering Perspective, Springer 2014, https://doi.org/10.1007/978-3-642-40888-5
43. Sabbaghi-Nadooshan, Reza, Abolfazl Malekmohammadi, and Mohammad Ayoub Khan. "Multicast Algorithm for 2D de Bruijn NoCs." In Embedded and Real Time System Development: A Software Engineering Perspective, pp. 235-249. Springer, Berlin, Heidelberg, 2014.
44. Gharbi, A., Khalgui, M., & Khan, M. A. (2014). Functional and operational solutions for safety reconfigurable embedded control systems. In Embedded and Real Time System Development: A Software Engineering Perspective (pp. 251-282). Springer, Berlin, Heidelberg.
45. Gautam, Ruchi, and Mohammad Ayoub Khan. "An efficient arbitration technique for system-on-chip communications." International Journal of Circuits and Architecture Design 1, no. 2 (2014): 193-207., 10.1504/IJCAD.2014.060701
46. 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.
47. Mohammad Ayoub Khan, A Q Ansari, Efficient Topologies for 3-D Networks-on-Chip, in book Multicore Technology: Architecture, Reconfiguration and Modeling, CRC Press (Taylor and Francis) U.K, https://www.researchgate.net/publication/258283178_Efficient_Topologies_for_3-D_Network-on-Chip
48. Verma, Renu, Mohammad Ayoub Khan, and Amit Zinzuwadiya. "Power and Latency Optimized Deadlock-Free Routing Algorithm on Irregular 2D Mesh NoC using LBDRe." International Journal of Embedded and Real-Time Communication Systems (IJERTCS) 4, no. 2 (2013): 36-49.
49. 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.
50. G Kaur, M Ayoub Khan Current differencing buffered amplifier an active element: a review of recent developments, Proceedings of the International Conference on Advances in Computing, Communications and Informatics, https://doi.org/10.1145/2345396.2345435
51. S. C. Tiwari, M. A. Khan, K. Singh and A. Sangal, "Standard test bench for optimization and characterization of combinational circuits," *2012 IEEE International Conference on Signal Processing, Computing and Control*, 2012, pp. 1-5, doi: 10.1109/ISPCC.2012.6224346.
52. Khan, Mohammad Ayoub, and Abdul Quaiyum Ansari. "Area-efficient programmable arbiter for inter-layer communications in 3-D network-on-chip." Central European Journal of Computer Science 2, no. 1 (2012): 76-85.
53. Ansari, A. Q., & Khan, M. A. (2012). A Journey from Computer Networks to Networks-on-Chip. IEEE Beacon, 31(1), 71-77.
54. Tyagi, Sapna, Preeti Sirohi, Mohammad Yahiya Khan, and Ashraf Darwish. "Industrial Information Security, Safety, and Trust." In Handbook of Research on Industrial Informatics and Manufacturing Intelligence: Innovations and Solutions, pp. 20-31. IGI Global, 2012. DOI: 10.4018/978-1-4666-0294-6.ch002

55. 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.
56. Khan, Mohammad Ayoub, and Abdul Quaiyum Ansari. "High-speed dynamic TDMA arbiter for inter-layer communications in 3-D network-on-chip." Journal of High Speed Networks 18, no. 3 (2012): 141-155.
57. Saeed, Saqib, Rizwan Ahmad, Zaigham Mahmood, and Mohammad Ayoub Khan. "Technology Support for Knowledge Management in Industrial Settings: Issues and Implications." In Handbook of Research on Industrial Informatics and Manufacturing Intelligence: Innovations and Solutions, pp. 211-226. IGI Global, 2012, DOI: 10.4018/978-1-4666-0294-6.ch009
58. Verma, Kumkum, Sanjay Kumar Jaiswal, and Mohammad Ayoub Khan. "Design of a high performance and low power 1Kb 6T SRAM using bank partitioning method." In 2011 International Conference on Multimedia, Signal Processing and Communication Technologies, pp. 56-59. IEEE, 2011.
59. M. Sharma and M. Ayoub Khan, "Energy and power issues in Network-on Chip," *2011 World Congress on Information and Communication Technologies*, 2011, pp. 1328-1333, doi: 10.1109/WICT.2011.6141441
60. 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.
61. 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.
62. Tyagi, S., Ansari, A. Q., & Khan, M. A. (2011, September). Extending Temporal and Event Based Data Modeling for RFID Databases. In International Conference on Parallel Distributed Computing Technologies and Applications (pp. 428-438). Springer, Berlin, Heidelberg.
63. Khan, Mohammad Ayoub, and Abdul Quaiyum Ansari. "Modelling and Simulation of 128-Bit Crossbar switch for Network-on-Chip." International Journal of VLSI Design & Communication Systems 2, no. 3 (2011): 213
64. 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.
65. Khan, M. Ayoub, and A. Q. Ansari. "From computer networks to network-on-chip." In International Conference on Nanoscience, Engineering, and Advanced Computing, pp. 28-33. 2011.
66. 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.
67. Khan, Mohammad Ayoub, and Abdul Quaiyum Ansari. "Quadrant-based XYZ dimension order routing algorithm for 3-D Asymmetric Torus Routing Chip (ATRC)." 2011 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC). IEEE, 2011.
68. Khan, M. A., & Ansari, A. Q. (2011, April). Low-power architecture of dTDMA receiver and transmitter for hybrid SoC interconnect. In 2011 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC) (pp. 350-354). IEEE.

69. Khan, M. A., & Ansari, A. Q. (2011, March). 128-Bit High-Speed FIFO Design for Network-on-Chip,”. In Proc (pp. 116-121).
70. Khan, Mohammad Ayoub, and ABDUL QUAIYUM Ansari. "A Review of Hyper-Torus based Topologies for Network-on-Chip." In Proc EEE International Conference on Emerging Trends in Computing (ICETC 2011), Coimbatore, 17-18 March 2011 , India
71. Ansari, A. Q., and M. A. Khan. "Parallel and dynamic virtual channel manager (VCM) for 3-D network-on-chip (NoC) router." Indian Patent JOURNAL 16 (2011): 07-38.
72. Sirohi, Preeti, Sapna Tyagi, and M. Ayoub Khan. "Industrial research-based approach for promoting higher education in developing countries." International Journal of Teaching and Case Studies 3, no. 2-4 (2011): 96-111., DOI: 10.1504/IJTCS.2011.039550
73. 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.
74. M. A. Khan, "Tracking Methodologies in RFID Network", in Radio Frequency Identification Fundamentals and Applications Bringing Research to Practice. London, United Kingdom: IntechOpen, 2010 [Online]. Available: https://www.intechopen.com/chapters/8482 doi: 10.5772/7995
75. S. Tyagi, M. A. Khan, and A. Ansari, "RFID Data Management", in Radio Frequency Identification Fundamentals and Applications Bringing Research to Practice. London, United Kingdom: IntechOpen, 2010 [Online]. Available: https://www.intechopen.com/chapters/8488 doi: 10.5772/8001
76. Sapna Tyagi, M Ayoub Khan, Active Data Warehouse approach for Radio Frequency Identification Applications, International journal of Advanced Computing (IJAC), Vol. 2(1), 2010, pp. 40-44, http://www.ijac.griet.ac.in/images/7v2i2j10.pdf
77. Khan, M. Ayoub, Manoj Sharma, and Brahmanandha R. Prabhu. "A survey of RFID tags." International Journal of Recent Trends in Engineering 1.4 (2009): 68.
78. Khan, M. Ayoub, and Videep Kumar Antiwal. "Location estimation technique using extended 3-D LANDMARC algorithm for passive RFID tag." 2009 IEEE International Advance Computing Conference. IEEE, 2009.
79. Khan, M. A., & Ojha, S. (2009, March). SHA-256 based n-Bit EPC generator for RFID Tracking Simulator. In 2009 IEEE International Advance Computing Conference (pp. 988-991). IEEE
80. Khan, M. Ayoub, Manoj Sharma, and R. Brahmanandha Prabhu. "FSM based FM0 and Miller encoder for UHF RFID tag emulator." 2009 IEEE International Advance Computing Conference. IEEE, 2009.
81. Khan, M. Ayoub, Manoj Sharma, and Prabhu R. Brahmanandha. "FSM based Manchester encoder for UHF RFID tag emulator." In 2008 International Conference on Computing, Communication and Networking, pp. 1-6. IEEE, 2008.
82. Khan, M. Ayoub, and Sanjay Ojha. "Virtual Route Tracking in ZigBee (IEEE 802.15. 4) enabled RFID interrogator mesh network." In 2008 International Symposium on Information Technology, vol. 4, pp. 1-7. IEEE, 2008.

83. M. Ayoub Khan, Ir. M K Awang, R Chowudhury, Y. P. Singh, “A public key infrastructure (PKI) for signing short message in GSM”, proceedings of the ICCCE’06, Malaysia, vol. 1, May 2006, pp:97-102.
84. 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.
85. A Darwish, S Tyagi, AQ Ansari, MA Khan, Radio Frequency Identification–Enabled Social Networks, pp.379-396, Knowledge Service Engineering Handbook, CRC Press, 2012
86. Tyagi, S., & Khan, M. A. (2013). Topologies and routing strategies in MPSoC. International Journal of Embedded Systems, 5(1-2), 27-35.
87. Saeed, S. (Ed.). (2013). Business strategies and approaches for effective engineering management. IGI Global.
88. Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi, Cybercrime: Introduction, Motivation and Methods, Cybercrime, Digital Forensics and Jurisdiction, Studies in Computational Intelligence 593, https://doi.org/10.1007/978-3-319-15150-2_1, 2015
89. Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi, Computer System as Target, Cybercrime, Digital Forensics and Jurisdiction, Studies in Computational Intelligence 593, D https://doi.org/10.1007/978-3-319-15150-2_2, 2015
90. Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi, Injection of Malicious Code in Application, Cybercrime, Digital Forensics and Jurisdiction, Studies in Computational Intelligence 593, https://doi.org/10.1007/978-3-319-15150-2_3, 2015
91. Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi, Attempts and Impact of Phishing in Cyberworld, Cybercrime, Digital Forensics and Jurisdiction, Studies in Computational Intelligence 593, https://doi.org/10.1007/978-3-319-15150-2_4, 2015
92. Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi, Sexual Harassment in Cyberworld, Cybercrime, Digital Forensics and Jurisdiction, Studies in Computational Intelligence 593, https://doi.org/10.1007/978-3-319-15150-2_5, 2015
93. Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi, Online Obscenity and Child Sexual Abuse, Cybercrime, Digital Forensics and Jurisdiction, Studies in Computational Intelligence 593, https://doi.org/10.1007/978-3-319-15150-2_6, 2015
94. Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi, Anonymity, Privacy and Security Issues in Cyberworld, Cybercrime, Digital Forensics and Jurisdiction, Studies in Computational Intelligence 593, https://doi.org/10.1007/978-3-319-15150-2_7, 2015
95. Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi, Strategies and Statutes for Prevention of Cybercrime, Cybercrime, Digital Forensics and Jurisdiction, Studies in Computational Intelligence 593, https://doi.org/10.1007/978-3-319-15150-2_8, 2015
96. Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, Sapna Tyagi, 419 Scam: An Evaluation of Cybercrime and Criminal Code in Nigeria, Cybercrime, Digital Forensics and Jurisdiction, Studies in Computational Intelligence 593, https://doi.org/10.1007/978-3-319-15150-2_9, 2015