Security and Privacy Concerns in IoT Devices and Attacks in Smart Cities

Xu Hwanwg

May 13, 2022

Security and Privacy concerns in IoT devices and attacks in smart cities

Xu Hwanwg

Computing Laboratory, Fudan University, China

Abstract:

The complex and interconnected nature of smart cities raises major political, technical and socio-economic challenges for the designers, integrators and organizations involved in managing these new entities. An increasing number of studies focus on security, privacy and risks within smart cities, while highlighting the threats related to information security and the challenges facing smart city infrastructure in managing and processing personal data. In this paper we focus on the security, privacy concern in IoT devices that are being used for attack in smart cities.

1 Introduction

Nowadays, the population of the regions is rapidly increasing. Several cities began to develop their own strategies towards the concept of smart cities to improve the quality of life and provide better services to citizens [1].

Many countries with population growth are spending a large amount of money on projects related to smart cities. For example, technologies related to smart cities enable life to manage its day-to-day operations to make people's lives easier. Smart city infrastructure includes many interconnected devices and systems to benefit people in a variety of applications such as smart healthcare, smart transportation, smart parking, smart traffic system, smart agriculture, and smart homes to name a few [2,3,4,5].

Information-based networking (ICN) is a model of networks, able to maintain packet delivery in unreliable environments. Therefore, ICN can be considered as an alternative to IP based networks in smart cities [6].

The incorporation of various low-cost smart devices such as sensors and actuators, and the rapid development of wireless communication technologies that enable small and low-cost objects to connect to the Internet, have further increased the spread of the Internet of Things (IoT) where physical things change into smart things in everyday life[7]. Combined with IP-based approaches such as those presented in the work of Shenget al, ICN solutions can be applied to developing the emergence of IoT and related applications. Information-centric networks have the advantage of being an concept for naming content and locating information in the architecture center 6 rather than relying on IP host identifiers.[8]

Cities are smarter and this may cause people to face tremendous security and privacy risks due to the nature of devices with limited resources, which makes the smart city vulnerable to various security attacks. These weaknesses may cause many cyber-attacks. In smart cities. For example, malicious attackers may produce false data while manipulating sensor data, resulting in a loss of control over highly intelligent systems [9-15]. In 2015, 230,000 people in Ukraine suffered a major power outage due to a hacker attack. Many devices with limited resources such as sensors and cameras, which collect and share sensitive data in smart cities, can also be vulnerable to malicious hacker attacks that threaten the security and privacy of people in smart cities [16-20]. Because of these cyber-attacks, home area information that is collected and controlled through smart homes can provide a way to uncover people's lifestyle. In terms of privacy, cloud computing can provide cost-effective services for processing and storing data [21,22]. However, there are some issues with cloud-based IoT applications such as lack of support for navigation, location awareness, latency, and security, which can be solved through a fog computing model [23]. Fog Computing addresses these challenges by providing computing services to users at the edge of the network, which in turn Reduces latency and enhances service quality However, security and privacy are two difficult problems in fog computing due to differences in fog computing and cloud computing that make security solutions for cloud services inappropriate for fog computing services available to users[24]. Various encryption techniques can deal with security attacks. However, these technologies are not suitable for resource-limited IoT devices in smart cities. One solution in this regard could be to offload additional security-related processes to a fog-based node, which can enable security and data analysis directly at the edge of the network [25-30].

According to IBM's definition, the smart city concept is based on three main characteristics called 'staged', 'interconnected' and 'smart'[31-36].

Equipped: This feature means a city covered by a set of devices such as sensors and actuators. Therefore, city platforms have access to reliable and real information with these devices [37-45].

Connected: It means that a smart city has a huge set of systems that collaborate to provide information from various sites and sources. It is then possible to create a link from the physical world to the real world using a precise mix of interconnected and equipped systems [46-50].

Smart: refers to a prepared and interconnected environment that uses information obtained from various systems and devices such as sensors to improve the citizens' quality of life.

2 Literature reviews

The complex and interconnected nature of smart cities raises major political, technical and socio-economic challenges for the designers, integrators and organizations involved in managing these new entities [51-67]. An increasing number of studies focus on security, privacy and risks within smart cities, while highlighting the threats related to information security and the challenges facing smart city infrastructure in managing and processing personal data [68, 69]. This study analyzes many of these challenges, and provides a valuable synthesis of the relevant main literature, and the evolution of the smart city interaction framework [70]. The study is organized around a number of key topics within smart city research: 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 comprehensive review provides a useful view on several key issues and provides the main direction for future studies. The results of this study can provide an informational research framework and reference point for academics and practitioners.

Privacy concerns and attacks in smart cities

Almost all aspects of personal privacy are likely to be at stake in a smart city; Sensitive personal information such as location, identity, habits and social interactions will be violated if it is not well protected. In order to give our readers a better understanding of privacy issues in a smart city environment, in the following, we review the important issues that were found or studied from the perspective of various smart applications [81-56].

Security threats and countermeasures

Like other wireless networks, intelligent transmission systems are also vulnerable to various security attacks and appropriate countermeasures are required to secure the respective applications. The main requirements for a secure vehicle network include availability that ensures data transfer within latency requirements using low-weight and lightweight encryption algorithms [87]. Confidentiality makes vehicle identity and data completely anonymous. Authentication is another major security feature that ensures messages are sent by a legitimate ITS station, surrounding traffic sites are properly verified and data attacks from malicious users are prevented. To determine appropriate data access control for various ITS terminals, delegation is a vital security requirement [88]. Moreover, data integrity and verification that the data has not been modified by a malicious user is another security challenge.

The list of security attacks, security requirements that pose a threat, and potential countermeasures are illustrated [89]. DoS attacks affect service availability and thus the quality of service for security applications. Attacks in this category include jamming attacks that transmit a noise signal onto the physical channel to increase interference levels and distort communications. On the other hand, spam attacks inject a large number of fake messages into the network to make the channel busy and unavailable [90]. Sybil attacks use false node identities to transmit fake messages that can cause network congestion as well as spread false information in the network [91]. Malware, spam, black hole, gray hole, sink hole, warm hole is some of the additional attacks targeting network availability [92]. To overcome most of these attacks, digital signature algorithms can be used.

3 Privacy Concerns in Smart Cities

3.1 SMART GRID

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].

3.2 CURRENT PRIVACY PROTECTION METHODS

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.

3.3 CRYPTOGRAPHY

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.

3.4 SUBSTITUTION CIPHER

The Kaiser code is one of the types of substitution code, but it is one of the simplest types where many complex codes can be created using the replacement code. For example, this table shows a simple substitution algorithm using the key 123 Plaintext A I T P E D I A Key +1 +2 +3 +1 +2 +3 +1 +2 Ciphertext B K W Q G G J C A more complex substitution algorithm can be used against each letter of the alphabet with another letter, not on the designation. For example, we use the following key:

The question is: Why did we choose the key (DKVQFIBJWPESCXHTMYAUOLRGZN) and does it have a specific rule? This key is chosen randomly and there is no specific rule for choosing it, but we try as much as possible to distribute the letters apart. For example: If we want to encode ait pedia using this algorithm, it will be in the form

Plaintext AITPEDIA Ciphertext DWUTFQWD Attempting to break the simple substitution algorithm is more difficult than Caesar's algorithm. While knowing the original letter corresponding to a blinded letter in Caesar's algorithm leads to knowledge of the remaining characters, the situation is completely different in the replacement algorithm as the range of values or attempts needed to break the algorithm is 26 x 25 x 24 x ... x 1, which equals 26! It is approximately equal to 4 × 1026 and is a large field that provides greater immunity to penetration. This method is not strong enough and the problem is that the language (whether Arabic or English) has repetition, as

the letters are not equal in use. Attempts to penetrate this algorithm are based on the character frequency of the original language, as it is calculated by testing a large number of texts. If we assume, for example, That the frequency of the letter e is 13%, so we calculate the frequency of the letters in the encrypted language. If we find that the letter t, for example, has a frequency close to this frequency, this often leads to that the letter t in the blind language is offset by the letter e in the original language. As an example, take the following text:
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX.
EPYEPOPDZSZUFPOMBZMJDFUDZ. In order to find out the original text, we calculate the most frequent character in the text, and for the sake of guesswork, we make P = e, Z = t, and by way of guessing also we make ZW = th so that it is ZWP = the, and after attempts we get the following text: it was disclosed yesterday that several informal but direct contacts have been made with political representatives in Moscow

4 Conclusion

As cities expand and grow, they have become dynamic smart homes. In fact, many governments launched smart city projects represents the best way to make the city smart. In fact, IoT can be applied in multiple scenarios such as building health monitoring using passive WSN networks, and environmental monitoring, for example. Gas concentration, water level of lakes or soil moisture, waste management, smart parking, carbon dioxide emissions reduction or autonomous driving. Achieving such goals requires an enormous number of connected objects. In fact, the number of connected objects is increasing exponentially, and it is estimated that 50 billion connected objects will be deployed in smart cities by 2020, however, this large number will open many risks and privacy issues, and in this work, we have provided an overview of the Internet. Things in the context of smart cities, and we discussed how they can enhance city intelligence, and we also identified weaknesses and risks associated with spreading and adopting the Internet.

Reference

1. 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.
2. 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

3. 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.
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. 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.
6. 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.
7. 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
8. 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.
9. 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.
10. 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.
11. 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
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. 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.
14. 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
15. 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

16. 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.
17. Khan, M. A. (2021). A formal method for privacy-preserving in cognitive smart cities. Expert Systems, e12855. https://doi.org/10.1111/exsy.12855
18. 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.
19. 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.
20. 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
21. 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.
22. 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.
23. 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.
24. 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.
25. 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
26. Rashmi Bhardwaj, Varsha Duhoon, Mohammad Ayoub Khan, Smart Technologies and Social Impact: An Indian Perspective of Contactless Technologies for Pandemic,
27. 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
28. 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
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