An Analysis on IoT Forensics: As a Use Case Amazon Echo System

Antino Francis (ubksa2018@gmail.com)
University of Atlanta, Chamblee, GA 30341, United States

Short Report

Keywords: Internet of things (IoT), Forensics, Amazon

Posted Date: March 11th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1439971/v1

An Analysis on IoT Forensics: As a Use Case Amazon Echo System

Antino Francis

University of Atlanta, Chamblee, GA 30341, United States

Abstract: We determine the identity of the Internet of things (IoT) such as sensors or anything that has a connection such as the router and the preservation of evidence needs to obtain evidence from its owners and after that we have an analysis phase in which some forensic tools are used The FTK computer is used in the electronic discovery process and finally it presents the investigators to obtain the results and reasons, Its importance is considered to be special for dialogue and scenario within the process, because Internet of things systems contain different settings, for example, forensic things in Amazon.

Keywords: Internet of things (IoT), Forensics, Amazon

1 Introduction

The Internet of thing (IoT) has emerged as many possibilities in our life such as healthcare, smart industry, security, and smart cities [1-13]. This rise has also opened the doors for security analyst to analyze the crime related to IoT. The forensic medicine is storing the evidence of convicts in the IoT, the number of intelligent people began to increase from simple billions to enormous billions, and the number of devices connected to the Internet, so that by 2022, the cybersecurity industry for the Internet of Things will include several sectors such as the military, It is more attractive to attackers, that is, it is possible to obtain data from a smart device or printer, and you can get distributed denial of service attacks and then it has become very important due to the increasing number of smart people, smart devices, and forensic medicine is known as the application of several tools and methods [14] . Samples are taken from evidence sources and it contains the same concept of traditional forensic medicine where it has a set of necessary stages, namely We identify the evidence, we save it, we start the analysis, and then we present it to the investigators when it is in the identification stage. We determine the identity of the Internet of things such as sensors or anything that has a connection such as the router and the preservation of evidence needs to obtain evidence from its owners and after that we have an analysis phase in which some forensic

tools are used The FTK computer is used in the electronic discovery process and finally it presents the investigators to obtain the results and reasons, Its importance is considered to be special for dialogue and scenario within the process, because Internet of things systems contain different settings, for example, forensic things in Amazon.

In recent years, the value of the electronic forensic system is summarized in that forensic medicine for the Internet of things has been the point of attraction for the Internet of things, and they must beware of it, because forensic medicine in all portable devices varies according to their uses and the nature of their work [15]. The importance of forensic medicine is very important and necessary due to the presence of the Internet in all devices, and evidence can be obtained through internal networks, the Internet of things and some servers. A model has been developed so-called forensic analysis and how to use , Illegal medicine is storing the evidence of convicts in the Internet of things, and then interrogating them has become very important due to the increase in the number of smart people. Or anything related, such as the router and the preservation of evidence, needs to obtain evidence from its owners, and after that the analysis stage we use some forensic tools such as used in the electronic discovery process and exposed to the investigators to obtain the results it to confront the investigation through a set of existing research tools depending on the type of data I have and because The volume of data can be large, so it is necessary to design to obtain the necessary and important data [16].

There are some approaches proposed by the writers and there are several Scientists have done Shancang Li, Kim-Kwang Raymond Choo Senior Member, IEEE, Qindong Sun, William J. Buchanan, and Jiuxin Cao ,By devising a number of techniques to achieve forensic medicine in the Internet of things, It categorizes the writers,IoT forensics into three zones: IoT zone, network, and cloud,Zone, where each zone is made up of numerous areas and forensics, Automated forensic management proposed by the authors,Device (FEMS) that has been configured to gather data from a system,Three-layered design, namely: vision, network, and software,Of layers. Nevertheless it is difficult for complex IoT networks to,For FEMS to investigate all IoT system states. From Zawoad et al.. A forensic-aware IoT (FAIoT) model was suggested, which enables the Proof gathered to be kept Activities for research. it is necessary to present the elements of evidence with the original coordination, because devices that identify, collect and preserve data and evidence when investigating are examples Amazon Echo. When determining the Internet device, questions must be answered, what is the scene of the crime, what time the crime took place, the location, etc. Then the method is presented to the Internet of things device in six steps, and we also create what is the device’s area, create a life cycle for the device, examine the device, and create access to

determine the possibility of confidentiality, authentication and licenses, And determining access to devices, all these methods are used by investigators and Internet things are used, but most of them contain a processor, a control unit and a memory (Rom, Ram) [17]. And wireless connection and may be equipped with CD, Also, what distinguishes the Internet of things is also the simple existence of a simple code without a system. I have traditional forensic tools such as FTK,DD The paper also explained how evidence is preserved, how it is extracted, and we have techniques AF, Lead to data overwriting and memory challenges can also be used Time Stomp2 for writing NTFS ,Except for stamps and their mods, we also have technology Amazon Echo(p) , It is a smart home assistant that is popular for its method of taking orders from users to control itself and Internet-connected sensors such as smart fryers, and we also have voice recognition technology Alexa in Most devices require a connection WIFI To be analyze Amazon Echo And its interactions are stored in the database SQlite ,And cache files are analyzed by Android An application is also used Windows ,ios 10.1.1 ,Alexa, Os X 10.10.5 Identifies encrypted connections. Untrusted communication authors are also detected API And web services, RESTful, Also, most researchers found that most of the data contain timestamps, Unix. The analysis was used to create a timeline of activities for the investigation ,Android, It is also very easy in the forensic of the Internet of things. Data is analyzed using the images of the second program through, Only delivery UART in Echo Also was used Alexa Pi , To build a file and copy it into several pictures of the cover, after that the data type and serial number are analyzed and by time, device data and addresses Wifi and Ip And also an address It also includes the username, password, and email address, as well as the language the data was obtained from Alexa Pi To obtain data related to the network device, information and account, it is possible to extract more detailed data using the two tools and physical methods, including the name of the device and the network Wifi Extracting the language and number immediately after the analysis is this command line that allows raw access to part of the memory areas Ic Also you can get a site picture . kernel Using the command line (ClI) u-boot Also can be used Zenmap To specify an address IP and Mac From Echo It is considered Ping, Also, the port sounds can be used to identify what all the open ports are on the devices. Also, all information can be obtained to identify the device by realizing the following software as well, Amazon Echo, Provide an ID for the results to use AVS , There is also a technique of analysis and examination, where information is displayed for both devices, the most important of which are the serial number and address mac , Also the parser can extract the name of the device we also use Echo An address that was set in Lieutenant's application Alexa , It provides weather forecasting and positioning also determines the location and weather information and identifies the device such as Google Maps and determines the geographical location such as the postal code for example

Amazon Echo It can store private conversations or audio signals as well as store the recordings on a server Amazon Alexa The time zone of the device is the key to determining the data with the timestamp. Defines particular audio files, such as Stop.mp3, and specifies the last time the audio files have been entered. to turn on the device. Also, there are several forms in this paper that use keywords such as echo, mac. Also, email addresses are found with user accounts and passwords.

2 Literature Review

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. Cybersecurity is that the inevitable drawback that has to be solved within the development of the net of Things[18-24]. 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 analyzes 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 [25,26,27,28]. 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[29-32].

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 [33,34]

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 Thing [35].

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[36-38].

Quick look to the different in Internet of Things (IOT) architectures: -

Number of Layers	**Major Technologies**
Three Layers	Sensing, Network, Application Perception, Network, Application Perception, Transportation, Application Perception, Network, Application Perception, Network, Service Perception, Network, Application
Four Layers	Sensing, Networking, Service, Interface Perception, Network, Support, Application
Five Layers	Field Data Acquisition, Access Gateway, Internet, Middleware, Application Perception, Network, Middleware, Application, Business

The attackers always take any chance to use the system weakness point to inject malware into the system through viruses, worms, Trojan horses, and spyware to deny service change data, and/or access confidential data or just to distrait the system. Because most of smart devices are not integrate will with each other, communication, protocols, applications, and services, the attacks appear to be malicious [39]. We categorize different attacks into eight classifications as Dr. Yang lu mentioned in his paper.

We have to shortly the IoT security schemes into 3 categories: Host Identity Protocol (HIP)-primarily based schemes, Datagram Transport Layer Security (DTLS)- primarily based schemes, and Capability-based Access management (CapBAC) schemes

In the end of this essay we have to know that the Internet of Things (IoT), is rising technology that change and improve the people life and make it easier ,not only People who get benefited , also organization, are based on (IoT) .Therefore, the author Dr. Yang Lu mentioned the most important points from his personal opinion in his research which are: on what does the Internet of Things system depend on ,the structure of (IoT) , and the types of penetration in the cyber space and also explained other important points in (IoT).

3 CASE STUDY

For the purpose of evaluating the ForKaS platform, the team developed a prototype that was evaluated using the IoT Forensic Datasic dataset from the 2017-2018 DFRWS Forensic Challenge3.

Simon is investigated in the case of the murder of his wife Betty, whose body was found on the floor of the house. The dataset contains forensic data obtained from several devices (a Raspberry Pi, a Smart Watch, a Samsung Smart Hub, two Samsung Note 2, a sensor) in addition to Amazon Echo Cloud Data, Google On Hub Diagnostic report, and MDS (Acme, Inc.) Smart home Network Dump. With this dataset the team built a Schema Pool using the schema builder which consists of several charts. As a result of analyzing the file using the initial ForKas model, it was found that the file stores sensor data in the Smart Hub network, so the most important file data was chosen which represents the device name, device ID, time, device status and status value.

A. Data analysis

The team built a Smart Hub network that includes two multi-purpose sensors, a motion sensor and a power outlet. They also installed the Smart Hub application – SmartThings Classic (v2.16.0) on a jailbroken iPad mini (IOS 9.3.5) and a rooted Samsung Galaxy S7 (Android 6.0).

The team built a Smart Hub network that includes two multi-purpose sensors, a motion sensor and a power outlet. They also installed on an Android device.

Once the Smart Hub application on any device is paired to the Smart Hub network, the data between that device and the Smart Hub will be synced.

After seven days of activities, app data was extracted from both devices.

B. Schema application

After that, they submitted an application to Panel Pool and the scheme was recommended, as it was taken with the highest score.

Once the most appropriate chart was presented, they downloaded the data obtained from the analysis of iOS and Android devices and applied the chart to this data.

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:

- 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, multilayered perception in space, inspired by the interconnections found in the visual cortex of the brain.

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[41]
- **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**.**

FUTURE DIRECTIONS

- **Honeypot development:** Expand the range of IoT simulators and handle massive amounts of inbound traffic [42].
- **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.

4 Conclusion

Due to more applications, the importance of IoT forensics will increase. We are connected to the Internet or some kind of network around us. (Such as a network for a private home or office). In other words, the evidence, Information may be collected from IoT computers, intranets, and applications, Any remote servers (in the cloud) and / or other IoT components, From the ecosystem. This makes the problem of timely identification difficult. Potential sources of evidence and obtaining evidence. This makes it difficult to decide the best time. Possible origins of data and evidence retrieval. We have thus introduced a forensic investigation model of the Internet of Things in this article. He clarified how to use it to direct the investigation, Echo of Amazon. A variety of possible research opportunities have also been listed. Identification of possible sources of evidence in a timely manner and obtaining proof. The type / format and age of the data which differ from one type to another. Since it is possible to offer IoT applications as services in It is possible to spread directories on the cloud platform through, Various cloud servers overseas, probably, Competence. Proper design is therefore necessary, Tools which can facilitate the acquisition. In addition to helping to draft legislation for policy makers, Facilitating the acquisition of remote data to ensure facts, Admissibility. We will need to build instruments or technologies that make it possible for us to. To satisfy the broad requirements for storage associated with, Space quest. We have to keep pace with new and evolving IoT products. Need for IoT design for forensic / off-the-shelf. In order to promote detection, systems, And the safe preservation of criminal data. That will be given for the investigation into the crime. So, we introduced the Internet of Things.

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] https://www.intel.com/content/www/us/en/products/details/processors.html

[15] Joseph B, Scaling for IoT Market Demands, https://www.digit.in/features/apps/scaling-for-iot-market-demands-34645.html, published on March 15, 2017

[16] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos. Context aware computing for the internet of things: A survey. IEEE Communications Surveys & Tutorials, 16(1):414–454, 2014

[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.