International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-5, June 2019

DDoS Risk in 5G Enabled IoT and Solutions

Deivanai Gurusamy, Deva Priya M, Barmura Yibgeta, Assabu Bekalu

Abstract: ***Some countries have started deploying 5G networks to meet the demands which include high bandwidth, low latency, high performance and high reliability. At the same time, Internet of Thing (IoT) based applications are increasing day by day. It is evident that 5G would enable more applications in IoT, including connected cars that optimize traffic. When 5G and IoT come together, considering security challenges would be indispensable.The existing researches have discussed various issues in 5G and the security risks associated with IoT. As finding solutions is crucial, the consequences of the most severe cyber-attack called Distributed Denial of Service Attack (DDoS)demand much attention.Hence, this paper presents a survey of the evolution of 5G, 5G-enabled IoT applications and the magnitude of DDoS attack in such applications. This survey assists in developing secured 5G enabled IoT applications by discussing various solutions to overcome DDoS attacks.***

Index Terms: 5G, Distributed Denial of Service, Internet of Things, Security.

I. INTRODUCTION

Currently, the next generation 5G networks are scaling to new heights in research. It would benefit the organizations by yielding success in business. According to Ericsson, the global telecommunication firm, there might be 1.5 billion 5G subscribers for enhanced mobile broadband between 2020 and 2024. The corporates Qualcomm and Intel are in the process of developing 5G modems suitable for smartphones and smart home devices. The telecommunications company Vodafone claims to be the first in starting the 5G trial, and the EE Enterprise is expected to launch the 5G network in the UK soon [1].

AT & T has launched 5G mobile hotspots in 12 countries [2], and Verizon's 5G Home is the world's first 5G network launched in 2018 [3] [4]. Australian 5G networks are gearing up to service and, Telstra and Optus are ready to offer their 5G commercial services on mobile broadband [5]. The South Korean telecoms havedeployed the world's first 5G service in 2018.

While 5G is on the way, Internet of Things (IoT) applications are everywhere, and it is expected to have much more Massive Internet of Things (MIoT) applications shortly. All those applications demand high bandwidth to handle data, voice and rich video generated by many IoT devices deployed in the environment. So, a promising

Technology which could support IoT applications with high bandwidth is the need of the hour. There comes a 5G network that promises to be ultra-reliable and ultra-efficient with high bandwidth [6] [1].

When these promising technologies strive together, security is the primary concern. Moreover, Distributed Denial of Service (DDoS) attack is threatening and its impact on 5G enabled IoT applications is likely to be more. A defense mechanism stronger than the existing ones is required [5]. Hence, this paper discusses about5G networks, 5G enabled IoT applications and the impact of DDoS on those applications. The paper also suggests some solutions to protect the network from such attacks. The paper is organized as follows. Section 2 describes the related work. Section 3 explains about 5G networks, while Section 4 describes the role of 5G in IoT applications. Section 5 describes the DDoS attack in 5G-enabled IoT applications, and Section 6 suggests a few solutions for a secure 5G enabled IoT. Section 7 concludes the paper.

II. RELATED WORK

Many researches have dealt with connecting IoT and 5G, and some of them have described the challenges involved in it. This section describes a few essential researches which give a broad idea about 5G technologies, the necessity of 5G for IoT applications and the challengeswith possible solutions.

Skouby and Lynggaard [7]have stated that IoT applications require cloud services that handle big data and Artificial Intelligence (AI) to process data with a better performance, which raises the need for 5G network. They have given a4-layered model which strongly recommends 5G networks for IoT applications.

Khan et al [8] have compared different generations of cellular technologies and have described the concepts and applications of 5G along with the security threats involved. The authors have stated that as 5G offers Internet Protocol (IP) based solution, it would be vulnerable to spooling, eavesdropping, masquerade and phishing attacks.

Mitra et al [9] have described the technologies proposed for enabling 5G which includes architecture, modulation schemes, multiple access techniques, energy efficiency techniques and protocol stack. They have also presented various works done towards the development of 5G.

Panhwar et al [10]have presented the evolution, benefits, traffic challenges and future considerations of 5G networks. In the survey by Akpakwu et al [11], the authorshave mentioned security as one of the biggest challenge.

Manuscript published on 30 June 2019.
***** Correspondence Author (s)
Deivanai Gurusamy*, Lecturer, Department of Information Technology, Bule Hora University, Bule Hora, Ethiopia, deivanaiguru@gmail.com
Deva Priya M, Associate Professor, Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, India, m.devapriya@skct.edu.in
Barmura Yibgeta, Lecturer, Department of Information Technology, Bule Hora University, Bule Hora, Ethiopia
Assabu Bekalu, Lecturer, Department of Information Technology, Bule Hora University, Bule Hora, Ethiopia

They have insisted on device identity and security mechanism deployment in IoT applications. They have also suggested authentication algorithms for the 5G enabled IoT network.

Li et al [12]have given in detail about wireless networks used for IoT applications and have reasoned out the need for 5G in IoT applications. Further, they have explained the architecture of 5G enabled IoT and the requirements. They have also discussed about the security and the privacy issues, and the research challenges in 5G enabled IoT.

Garcia et al [13]have proposed a prototype called 5G-aware traffic filtering which offers protection against the cyber-attacks. This filtering method uses Deep Packet Inspection (DPI) function to determine whether to permit packet transmission or not.

Ahmad et al [14]have given an overview of security and privacy challenges in 5G. As cloud, Software Defined Networking (SDN) and Network Function Virtualization (NFM) concepts enable businesses and users to get more benefits through proper network management and effective data services, the authors have analyzed the various security challenges in these concepts with 5G. From their research, it is clear that DDoS is one of the security challenges in all three concepts (cloud, SDN, NFV). They have propounded solutions to improve security in 5G networks. Specifically,they have dealt with providing security against the DDoS attack at a centralized control point.

Thispaper discusses particularly about DDoS attack in 5G enabled IoT applications as it is widespread in the Internet world andonly a few researchers have discussed on this.

III. 5G - The Next Generation Network

5G is the fifth-generation radio access technology from telecommunication service. It utilizes high-frequency millimeter wave technology that allows transmission of data faster than the 4G technology [15]. It promises to provide higher download and upload speeds, faster streaming of online content, ultra-quality video and audio calls, ultra-reliable mobile connections and support a massive number of IoT devices [5] [16]. Though 5G is a successor of 4G, it will not replace 4G overnight. Both the technologies would exist together for some more years.

Table 1 shows how 5G differs from 4G [8] [9] [10].

Table 1 Comparison of 4G and 5G networks

Generations vs. Features	4G (2010)	5G (2020) (Promises to be)
Technology	LTE, LTE-A	LTE-M, New Radio (NR)
Radio Convergence	Limited	Improved
Network Latency	Low (30-70ms)	Ultra-Low (below 1ms)
Network Speed	High	Ultra-High
Network Capacity	High	Ultra-High
Traffic	Data, Voice, Video	Mission Critical data and video and voice
Data rate	50-100Mbps	10Gbps
Energy Efficiency	High	High (Equal to 4G)
Multiple access technique	Orthogonal Frequency Division Multiple Access	Non-Orthogonal Multiple Access (not standardized yet)
Connection density	High	Ultra-High
Spectrum efficiency	High	Ultra-High
Mobility	High	Ultra-High

Ronan Dunne, Executive Vice President, Verizon have stated that 5G would provide $12.3 trillion of global economic output and offer 22 million jobs worldwide by 2035 [17]. Paul Bevan, research director for Bloor, an IT Infrastructure has mentioned that mobile online gaming, video streaming and virtual, and augmented reality would be the initial targets of 5G [18].

The challenges of 5G networks are migration from 4G to 5G, establishment of 5G business models, data interoperability, setting up network core and managing operation across multiple spectrum bands [19]. The forecasted benefits are better connectivity, reduced latency, high speed, energy efficiency and cost efficiency [10] [18] [20]. With these benefits, 5G technology will rule the world in a few years.

Figure 1 shows some applications that would be benefited through 5G.

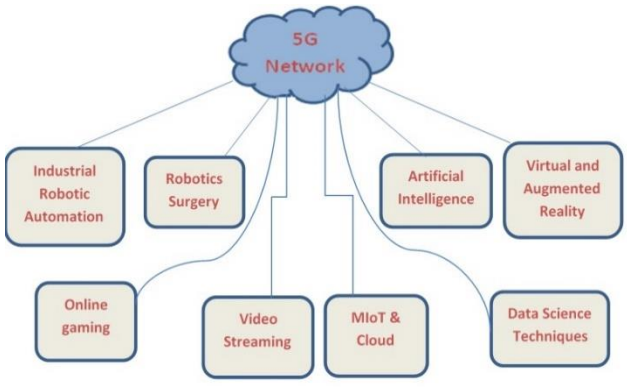

Figure 1 Applications of 5G

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

IV. 5G - ENABLED IOT

Internet of Things (IoT) is a technology that includes devices which share data on the internet. Companies, cities, and homes are changing to be smart with IoT. It increases the number of things connected on the Internet day by day, and it could be more than 21 billion IoT devices by 2020 [21]. These devices make use of cellular technologies such as 2G/3G/4G, Wi-Fi and Bluetooth which have not yet been optimized for these applications [12].

The Long-Term Evolution (LTE) technology from 4G could be helpful, but the LTE technology used in mobile phones and IoT are different. So, cellular network providers have launched Cat-M1, an LTE network, especially for IoT applications.

Verizon has launched Cat-M1 in 2017, which is believed to be a technology that consumes less power. Also, Cat-NB1, a narrowband IoT is proposed as a Low Power Wide Area (LPWA) technology that connects the low-power devices to the mobile network from anywhere. Better solutions for IoT are being developed [22], and the hype of 5G improves the expectations towards 5G-enabled IoT applications which may consume less power and involve less latency.

All the IoT applications do not require 5G networks. For example, a few applications that make periodic updates do not consider the latency issues, but 5G network emphasizeson low latency. However, a 5G network can support IoT applications with low latency and high reliability.

Mainly, it will handle large amount of data generated by millions of IoT devices at the background, while users enjoy the benefits of 5G enabled applications in real-time. The deployment of IoT applications in 5G networks may take some more time. In June 2018, the telecom industry association, 3rdGeneration Partnership Project (3GPP) published Release 15 that supports 5G for smartphones and cellular networks. In addition, 5G is meant not only for Low Power Wide Area Network (LPWAN), but also for IoT applications that fall into the category of Ultra-Reliable Low-Latency Communications (URLLC) [18].

So, for 5G-enabled IoT applications, release 16 and 17 are approaching later this year. Machina research forecasts that IoT will account for one-quarter of the global 41 million 5G connections in 2024 [23]. The high data rate, high scalability, reliability, security, low latency, connection density and long battery life are the requirements for 5G-enabled IoT applications [12].

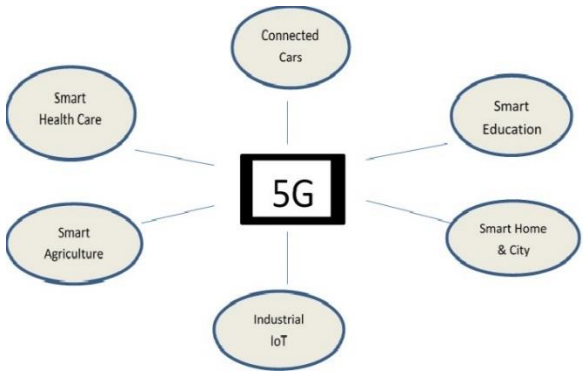

Figure 15G- Enabled IoT Applications.

Figure 2 shows some of the 5G-enabled IoT applications such as connected cars, health care monitoring, smart education, smart city, smart home, agriculture and industrial IoT [24].

Though the technology is not widely used at present, a significant revolution with a world filled with 5G enabled IoT applications with no cabling requirements, ultra-low latency, ultra-reliability and ultra-efficiency is expected in the near future [6].

V. 5G –ENABLED IOT AND DDOS

DDoS attacks are beneficial to hackers. Flooding leads to DDoS, even at the firewall. These attacks are executed for ransom to pull down business or executed against the government. This kind of attack is encouraged among attackers since the tools and technologies required for those attacks are readily available and inexpensive [25].

The majority of DDoS attacks are sub-saturating with low-threshold. They often 'Fly under the radar' of legacy DDoS protection [26]. Also, Cisco has estimated that the number of DDoS attacks would exceed 1 GB of traffic per second and will soar to 3.1 million by 2021 [27].

IoT applications are using millions of devices which are less secure. It turns out to be the advantage for the attackers to flood the IoT environment. The growth in the number of IoT devices eases the work of cybercriminals to facilitate DDoS attack.

In 2016, the world confronted Mirai, a malware which affects IoT devices connected to the Internet and turned them into a botnet to trigger DDoS attack [21]. Some of the dropped malwares include mirai.x86, sora.x86, miori.x86, hoho.x86 from Mirai family and DEMONS.x86 from Gafgyt/Bashlite family. Majority of these attacks are hosted in the US, Italy, UK, Germany and Netherlands [27]. So, the enterprises that develop IoT applications must be prepared to deal with these threats.

When 5G is in place, IoT becomes MIoT with billions of devices that use 5G Radio Access Network (RAN). This could increase the possibilities of RAN resource overload by DDoS attacks [28]. To top it all, the 5G network providers are also the targets of those kinds of attack.

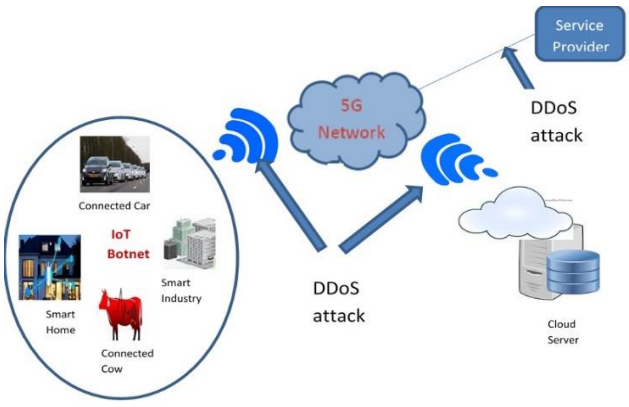

Figure 3 DDoS Attack Scenario in 5G-enabled IoT Environment

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Figure 3 shows the DDoS attack scenario in 5G-Enabled IoT environment.

VI. SOLUTIONS TO SECURE 5G ENABLED IOT

As far as security is concerned, 5G itself comes with some solutions. It introduces the concept called 'Network Slicing', where the network is segmented for quick mitigation of attacks. Also, it provides visibility and control elements that clearly shows the network operators how the application behaves to take control to protect the network [28]. However, much research is carried out to prevent DDoS attacks. Some of the solutions that are suggested to protect the IoT environment from a DDoS attack are listed below.

Solutions that are not encouraged

The following solutions are not entertained.

- **Scrubbing Centres:** When an attack is identified with sample thresholds, the traffic is diverted to a specific data center where the packet is inspected, the content with the attack is removed and the original data is allowed to pass through the network. This kind of solution is not feasible due to factors like high cost, reduced quality, inaccuracy and the familiarity of hackers about the sampling mechanism [25] [26].
- **Inline Systems:**It is designed for enterprises, but it does not contain solutions for the attacks in outbound traffic [25].

Solutions suggested

The following solutions are suggested.

- **Machine Learning (ML)Approach:** Machine Learning (ML)approach can be used to detect attacks. For example, an approach developed by Allot circumvents attacks through an automated solution which is integrated with Deep Packet Inspection (DPI) function that detects even unfamiliar attacks in both inbound and outbound traffic. This approach does not require high-cost infrastructure set up and is rapid [25].
- **Real-time Threat Detection:** This solution may be helpful to prevent DDoS attacks [27]. For example, Sean Newman, Director of Product management for Corero Network Security, recommends 'Corero' as a solution to DDoS attack. He ensures that the solution would help organizations to comprehend 5G tsunami attack as the solution is always on, automatic and real-time [26].
- **Automated Signature Extraction (ASE):** ASE [27] is a kind of solution by which the organizations can defend themselves from attacks.
- **Security as a Service (SaaS):** SaaS [13] is a kind of service provided by cloud providers. Itenables service providers and enterprises to protectthe network from attacks.
- **Encapsulation-aware Traffic Filtering Method:** This method uses DPI and integrates the filtering mechanism with the security architecture of 5G [13].
- **Signaling Storm Detection and Mitigation Function:** This function is added to the central unit of the network so as to protect it from attacks [28].
- **Cryptographic Algorithms:** These algorithms are capable of protecting IoT networks and are faster than legacy algorithms [28].
- **Router Security:** The IoT devices do not have any security software running in them. The router that connects devices may come up with an enhanced security mechanism, since it is the gateway that lets the devices to communicate with each other on the Internet. Router manufacturers are very much concerned inproducing security-enabled routers.
- **Device Management and Secure Bootstrapping:** By verifying the location of the devices and the platform where they are used, IoT security can be enhanced [28].
- **Authorization and Access Control:** It provides access control to IoT resources [28].
- **Application End-to-end Security:** It is implemented in the application layer [28].

VII. CONCLUSIONS

The evolution of cellular technology advances with 5G. Many enterprises are working on launching 5G services, which will take businesses to the next level. Though the technologies for the 5G network are not yet standardized, it is expected to offer high bandwidth, reduced delay and high performance. These advantages of 5G enable the Massive IoT (MIoT) applications, which in turn provide opportunities for the DDoS attacks. Hence, this paper has thrown lighton the impact of the DDoS attacks in 5G-enabled IoT applications and has provided an overview of solutions to protect the IoT environment from the DDoS attack. Among the solutions suggested, the Machine Learning (ML) based approach may provide an efficient environment, where DDoS attack will be drastically controlled. Further, the research may be extended to analyze the techniques of ML in developing an optimized IoT application with 5G network.

REFERENCE

1. H. Williams, "5G and smart cities trends for 2019," 3 January 2019. [Online]. Available: https://www.computerworlduk.com/iot. [Accessed 5 March 2019].
2. B. Hesse, "Here's Your Cheat Sheet for Verizon's New 5G Data Plans," 14 March 2019. [Online]. Available: https://lifehacker.com. [Accessed 11 March 2019].
3. K. Finley, "5G is coming for real, but it will cost you," 13 March 2019. [Online]. Available: https://www.wired.com/story. [Accessed 28 March 2019].
4. "What is 5G," Verizon, 2019. [Online]. Available: https://www.verizon.com/about/our-company/5g. [Accessed 11 March 2019].
5. A. Choros, "5G in Australia: Everything you need to know," 2019. [Online]. Available: https://www.whistleout.com.au. [Accessed 11 March 2019].
6. M. Koziol, "MWC Barcelona 2019: The Biggest Changes that 5G will bring to the IoT will be invisible," 28 February 2019. [Online]. Available: https://spectrum.ieee.org/telecom/wireless. [Accessed 5 March 2019].
7. K. E. Skouby and P. Lynggaard, "Smart Home and Smart City Solutions enabled by 5G, IoT, AAI and CoT Services," in International Conference on Contemporary Computing and Informatics, IEEE, Mysore, India, 2014.
8. M. H. Khan and P. C. Barman, "5G-Future Generation Technologies of Wireless Communication "Revolution 2020"," American Journal of Engineering Research, vol. 4, no. 5, pp. 206-215, 2015.

9. R. M. Mitra and D. P. Agarwal, "5G Mobile Technology: A Survey," ICT Express 1, ScienceDirect, Elsevier, vol. 1, no. 3, pp. 132-137, 2015.
10. M. A. Panhwar, M. S. Memon, S. Saddar and U. Rajput, "5G Future Technology: Research Challenges for an Emerging Wireless Networks," International Journal of Computer Science and Network Security, vol. 17, no. 12, pp. 201-2016, 2017.
11. G. A. Akpakwu and G. P. Hancke, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," IEEE Access, vol. 6, pp. 3619-3647, 2018.
12. S. Li, L. D. Xu and S. Zhao, "5G Internet of Things: A Survey," Journal of Industrial Information Integration, ScienceDirect, Elsevier, vol. 10, pp. 1-9, 2018.
13. P. S. Garcia, J. M. A. Calero, Q. Wang, J. B. Bernabe and A. Skarmeta, "5G NB-IoT: Efficient Network Traffic Filtering for Multitenant IoT Cellular Networks," Security and Communication Networks, Hindawi, vol. 2018, pp. 1-21, 2018.
14. I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Yianttila and A. Gurtov, "Overview of 5G Security Challenges and Solutions," IEEE Communications Standards Magazine, vol. 2, no. 1, pp. 36-43, March 2018.
15. M. Frankel, "What is 5G," 2019. [Online]. Available: https://www.fool.com/knowledge-center/what-is-5g.aspx. [Accessed 15 March 2019].
16. M. Moore, "What is 5G? Everything you need to know," 15 March 2019. [Online]. Available: https://www.techradar.com/news. [Accessed 15 March 2019].
17. Ronan Dunne, Verizon Wireless, "What is 5G," 02 01 2019. [Online]. Available: https://www.verizon.com/about/our-company/5g/what-5g. [Accessed 15 March 2019].
18. B. Violino, "How 5G can unlock IoTs potential," 16 January 2019. [Online]. Available: https://www.zdnet.com/article/how-5g-can-help-unlock-iots-potential. [Accessed 15 March 2019].
19. V. Gandhi, "5G to become the catalyst for innovation in IoT," 13 April 2018. [Online]. Available: https://www.networkworld.com/article/3268668/5g-to-become-the-catalyst-for-innovation-in-iot.html. [Accessed 15 March 2019].
20. "How 5G will help advance IoT Technologies," [Online]. Available: https://internet-of-things-innovation.com/insights/the-blog/5g-advances-iot-technologies.
21. Symanovich, Steve, Symantec, "The Future of IoT: 10 Predictions about the Internet of Things," [Online]. Available: https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html. [Accessed 15 March 2019].
22. Z. Supalla, "What's so special about 5G and IoT?," 20 July 2018. [Online]. Available: https://www.networkworld.com/article/3291778/what-s-so-special-about-5g-and-iot.html. [Accessed 15 March 2019].
23. "5G means Internet of Things," [Online]. Available: https://internet-of-things-innovation.com/insights/the-blog/5g-means-internet-things. [Accessed 15 March 2019].
24. "IoT Relation and Impact, Alliance for Internet of Things Innovation," 2018. [Online]. Available: https://aioti.eu/wp-content/uploads/2018/06/AIOTI-IoT-relation-and-impact-on-5G_v1a-1.pdf. [Accessed 15 March 2019].
25. M. Schachter, "DDoS & 5G: The Bigger the Pipe, the Stronger the Threat," 26 June 2018. [Online]. Available: https://www.allot.com/blog/ddos-5g-the-bigger-the-pipe-the-stronger the Threat. [Accessed 23 March 2019].
26. Sean Newman, Corero Network Security, "5G Will Increase DDoS Attack Risk," 10 December 2018. [Online]. Available: https://www.corero.com/blog/905-5g-will-increase-ddos-attack-risk.html. [Accessed 15 March 2019].
27. Hmad Nassiri, A10 Networks, "IoT and DDoS attacks -A match made in heaven," 1 March 2019. [Online]. Available: https://www.a10networks.com/blog/iot-and-ddos-attacks-a-match-made-in-heaven. [Accessed 15 March 2019].
28. "The Evolution of Security in 5G, 5G Americas White Paper, (2018).," October 2018. [Online]. Available: http://www.5gamericas.org/en/resources/white-papers/. [Accessed 11 March 2019].

AUTHORS PROFILE

Deivanai Gurusamy received her B. Tech and M. Tech degrees from Anna University, Chennai and Anna University, Coimbatore, India in 2005 and 2011 respectively. At present, she is teaching at Bule Hora University, Ethiopia. She is also a CISCO Certified IT Professional. Her knowledge and expertise have been duly recognized and is being invited to deliver Guest Lectures in different educational institutions. Her work has been published in various International Journals and Conferences. Her research interests include Wireless Sensor Networks, IoT and Cloud Computing.

M. Deva Priya received her Master's degree in 2007 and her Ph. D in 2015 from Anna University, Chennai. She is currently working as Associate Professor in the Department of Computer at Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India. Her research interests include Wireless and IoT Networks. She has published more than 45 papers in Journals and Conferences. She is a life member of ISTE & ISRD, member in IAENG and Senior Member in UACEE.

Barmura Yibgeta is currently working as a Lecturer at Bule Hora University, Ethiopia. He received his B.Sc degree in Information Technology from Jimma University, Ethiopia in 2013 and M. Tech degree in Computer Science and Engineering from Symbiosis Institute of Technology, Pune affiliated to Symbiosis International University, Pune, India in 2016. He has published papers in International Journals and Conferences. His research and publication interests include AHP, System dynamics modeling, Networking and Human Computer Interaction.

Assabu Bekalu received his B. Sc degree in Information Technology in 2014 from Debre Markose University, Ethiopia and M. Sc degree in Information Technology in 2017 from Bahir Dar Institute of Technology, Ethiopia. Currently, he is working at Bule Hora University, Ethiopia. He is into teaching since 2014 and has published papers in International Journals and Conferences. His research interests include Expert Systems and Networking.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)