Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

The Role of IOT and Cyber Warfare in Developing the Health Care Devices

Dr. Bhupendra Kumar
Professor, College of Business & Economics, Debre Tabor University Ethiopia
Email- drbkumar@dtu.edu.et
Addisu Worku Bezabih
Asst. Professor , Dean, Electrical and computer Engineering
Mail id. addisuworku@dtu.edu.et
Dr. Yagnam Nagesh
Professor , IT Department, Debre Tabor University , Ethiopia
naheshyagnam1@dtu.edu.et
Dr. Balachandra Pattanaik
Professor, Department of Electrical and Computer Engineering,
Wollega University, Ethiopia
Email: balapk1971@gmail.com
Dr. Umamaheswari K
Assistant Professor, Business Administration, Kabridhabar University Ethiopia uma@kdu.edu
Dr. Vidhya K
Assistant professor, LEAD College of Management, Dhoni, Kerala.
vithyakannanpsg@gmail.com

Article Info
Page Number: 1185-1194
Publication Issue:
Vol. 71 No. 3s (2022)

Abstract: The healthcare system of today is considered to be one of the most vulnerable systems to cyber-attacks. It is because the healthcare system handles sensitive data like payments, the history of a patient as well as private patient information, and the list goes on. When it comes to cyberattacks, healthcare systems cause significant harm to both organizations and patients. Due to the increased demands for high-quality healthcare and the increasing cost of care, ubiquitous healthcare is seen as a technology-based solution to tackle global health problems. Particularly, the recent advancements in the field of the Internet of Things have led to the creation of the Internet of Medical Things (IoMT). Although these inexpensive and widespread sensing devices could transform reactive healthcare into preventative the privacy and security concerns associated with these devices are often ignored. Since medical devices collect and process extremely sensitive personal health information these devices as well as their connected communications must be extremely secure to safeguard the privacy of the patient. However, the miniature IoMT devices are very limited in computing power and a few security options are available within these devices. Furthermore, with the wide usage of IoMT devices managing and ensuring security of IoMT devices is extremely challenging and constitute the primary problems that hinder the use IoMT IoMT to use in clinical settings. In this paper, security and privacy issues and threats, as well as the requirements and research directions for the future in the area of IoMT are examined, giving an overview of most recent methods.

Article History
Article Received: 22 April 2022
Revised: 10 May 2022
Accepted: 15 June 2022
Publication: 19 July 2022

Keywords: Healthcare systems, survey, Security, privacy, Internet of Medical Things, IoMT

I. Introduction

Cyber-security is a current research phenomenon and has applications in a wide range of fields such as military branches, governmental services and banking, education and healthcare software engineering, transportation and other services. In the past, banking was the most vulnerable sector, however, the healthcare sector is now the frontrunner in cyber-attacks. The majority of Cyber-Safety systems are based on an aspect of the Internet of Things. It is where IoT devices are a part of the problem of the mechanisms of data exchange. There are numerous issues in this area. The (IoT) connected physical world and the Internet patient information is collected from a variety of sources within IoT healthcare systems, and processed within the context that is the Electronic Health Record (EHR) can be shared via the internet using cloud computing. The clinical Health Record (EHR) is a full collection of information about clinical health that differentiates patients. It also comes in an electronic record format which can be shared with various areas of healthcare can be shared across different areas of healthcare [1]. It contains a variety of information like the patient's ethnicity, medical history and the results of treatment, and diagnostic examinations. There is also some patient billing information [2]. The requirements in the healthcare industry are extremely important and require secure security. Healthcare facilities also employ the form of device IoT and vary in their design. This is why these types of systems are not based on security mechanisms that are standard. Some of the techniques are created completely from scratch but with certain changes to the existing systems, they are utilized. So, the healthcare system should be tightly controlled and protected from any type of cyber-criminals or threats. The entire report discusses the most significant threats posed by the healthcare sector.

PMDs are also known as personal medical devices. (PMDs) are tiny electronic devices with only the most basic of resources. They're equipped with basic hardware and small firmware. They are becoming more famous and are expected to increase to 17.7 billion before the close of the year. PMDs help patients remain in good health and remain independent for longer durations of time, and lessen the need to provide assistance to their patients. They are usually able to wirelessly communicate with the base station that lets you access medical records on devices, check the health on the gadget, modify the parameters, or even update the software on the gadget. Wireless devices are vulnerable to cyber security threats, and also cause privacy and security issues for patients. The variety of attacks that target medical devices can lead to privacy breaches due to eavesdropping, integrity and security issues caused by modifications to messages, and access problems due to battery-draining attack which have been discovered by security researchers [5, 6]. There are various ways to counter these kinds of attacks. One of the main challenges in the development of solutions for medical devices is the limitation of resources for these devices to allow them to ensure security measures are in place. Any communication or activity that reduces battery life could be detrimental to performance and, consequently, the introduction of cryptographic security for your communications is a major problem. Even for devices that aren't implantable, the high-end cryptography needed to secure communications are not available on the platform of the

device. This is the reason why the use of light cryptography on these devices has become an increasingly popular research field in recent years [7]. The study of personal medical devices has been centred on the home network that allows medical devices to be capable of connected to the central station or gateway, which allows healthcare practitioners to access data over the internet. Medical gadgets will someday become part of the Internet of Things (IoT).

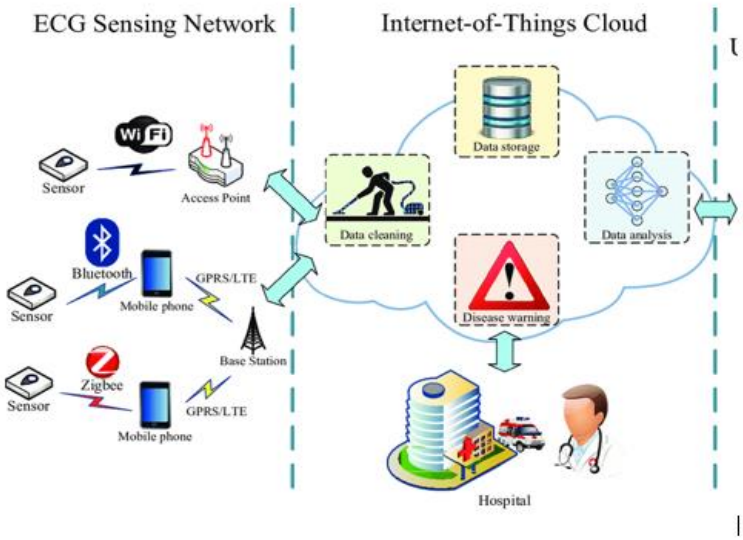

Figure 1: Architecture of IoT Based Health Monitoring Systems

The picture shows three networks where the medical device is connected to the patient's personal network, which is controlled by the patient as well as the hotspot that is open. Mobility and communication are utilized to assess the health condition of the patient throughout time. The data is saved in a cloud-based system where the patient has been registered. The medical device is registered with an address for the cloud-based system. Cloud-based solutions save information in the Personal Health Record (PHR) database that can be accessed through the institution or primary care physician the patient is affiliated with. Cloud-based services offer an online interface that allows patients to define the guidelines that permit access to the PHR data that is generated from their devices for medical purposes. An approach to integrating data from PMDs into an online health record using policies based on fine-grained disclosure is explained.

II. Related survey

Seyedmostafa Safavi, Ahmad Moaaz Meer, Ed Keneth Joel Melanie and Zarina Shukur et al [8]. They have proposed a data-related healthcare system that requires security because of the volume of data stored, it is essential to have an improved method of security to protect privacy and security. These methods can provide secure data storage for Smart Healthcare. Also, they can protect the things that are vulnerable and could cause the loss of information with the help of cyber-attacks. Blockchain is viewed as an option to improve privacy and security in digital healthcare. With blockchain-based technology, how can we create the best platform for the future of health care.

I M Skierka et al [9]. suggested that healthcare is transformed to digitalization day-to-day and also poses a risk or is dangerous to patient data. Since the majority of the reports of any diagnosis or health-related reports for a patient are created online. Additionally, data transfer is done online. In this article, the author has proposed the cybersecurity risks and threats to data stored in the healthcare sector. The types of risks are a few of the incidents that have been caused by medical devices. Certain vulnerabilities could cause major problems in the health sector.

Anastasiia Strielkina, Vyacheslav Kharchenko, and Dmytro Uzun et al [13]. They proposed a brand-new technology called the Markov model. With this model, users are able to securely connect their accounts via IoT devices which are directly interacted with by machines and humans and with this Markov model, users can protect the information that is transmitted over the internet or, it could be said that they are data is online. We are committed to the implementation of the security systems and safeguards in healthcare IoT devices, and the combination of these results through this article and the upcoming devices, taking into consideration accuracy as well as safety and security criteria and issues.

Aysha K. Alharam, and Wael El-madany et al [17]. Based on the rapid technological advancement, various types of research are conducted in the field to show the challenges and issues. Find solutions to these issues and confront problems, too. Since technology has become a part of our lives in all regions. A variety of research projects are planned to ensure data security and security in the field of IoT devices, mainly in the realm of healthcare-related applications.

Indrakshi Ray, Bithin Alangoty, Shilpa Nairy, and Krishnashree Achuthan et al [21]. They have proposed a Remote Health Monitoring, which is an IoT technology that works with the help of sensors and smartphones, doctors or healthcare organizations collect the details about patients' health and current condition or other important variables. The RHM system is built using IoT devices. They also discuss security concerns in the RHM.

III. Security Risks in Healthcare Sector

Healthcare applications are extremely sensitive software and the health data are crucial and more difficult to protect than other kinds of information and software due to the fact that they must be extremely secured [33. A variety of threats are a possibility for healthcare systems and they differ in the causes they cause and their resolutions. This article highlights the security risks that exist. Security risks include impersonation, eavesdropping and man-in-the-middle.

Eavesdropping is often referred to as an attack of sniffing, which is a method by which a person attempts to cut evidence that is transmitted via smartphones, computers, or other devices of the networks. Eavesdropping exploits unsafe transport methods to get in touch with the data that is spread and also established. It's difficult to detect Eavesdropping threats since they do not let net communications appear strangely operating.

Impersonation refers to the act of attempting to use a reason or to deceive an individual. Impersonation attacks are a kind of cyber-attacks where attackers attempt to use emails to pretend to be an individual or a company to gain access to confidential and private information.

Man-In-The-Middle

Man-in-the-middle attacks (MITM) can be described as a common attack where the hacker transmits secretly and possibly alters the communications between two people who believe they are communicating directly. [4]. To stop threats to health care systems different security measures are required to stop ransomware attacks of all types. Use a secure security framework and an effective model for encryption of medical data and encryption.

IV. Cyber security requirements

Cyber security needs are a collection of traditional security rules that guarantee the security of information, patient and the system by utilizing two primary elements: CIA Triad and non-CIA. Cyber security allows users to protect and guard healthcare systems that are based on IoT against attacks and threats. CIA trinity ensures the security of data for IoT by ensuring security, confidentiality and availability. Non-CIA is a different part of cyber security requirements that includes seven key features, including authorization, authentication privacy, accountability, auditing, and no-repudiation. The terms and features that are associated with cybersecurity requirements are listed below.

Cyber resiliency requirements

Cyber resilience (system resilience) is being viewed as a prerequisite for healthcare systems based on IoT to guard against unpredictability, inexplicably or unexpected threats. NIST standards define an effective cyber-resilient system as having the capability to prepare for unexpected hazards, adjust to the changing environment and withstand and recover swiftly from deliberate and accidental attacks, as well as natural disasters. System resilience must make sure that the security plan safeguards the system, network or data from any threat or loss. Cyber resilience features are divided into six primary categories that include reliability, maintainability, performance, safety, survivability and security of information. It is important to note that the requirements for cyber resilience overlap three aspects of cyber security such as confidentiality, availability and integrity.

There are many possible risks for medical devices that could result in the loss of Confidentiality and Integrity as well as accessibility. However, the most commonly cited examples are flaws or defective firmware and software. Writing software that is free of security concerns is not easy. In many cases, software developers haven't been properly trained to create secure software and are not aware of the dangers. In many instances, the software hasn't been tested to determine security concerns. Unconfigured network services. This may be the result of using insecure connections to the internet which could result in patient information being sent in plain text. Criminals could exploit the open networks and utilize them as a way to gain access to the device. Privacy and security issues like the use of weak passwords or excessive access rights where users can gain access to administrative features. It is not uncommon to find passwords recorded and taped to devices! The passwords can even become "hard-coded" in a device and make it easy for hackers to retrieve them. Poor data protection. This could be due to the lack or ineffective use of encryption for data. When used correctly, encryption is an effective way to protect data when it is in transit (i.e., in the process of is transmitted through the network). Most data security issues result from improper use of encryption keys as well as inadequate technical implementations. Incorrect removal or destruction of the device that has onboard memory that still contains patients' information. The safe disposal of the device needs

to be considered in the cost of ownership as well as the disposal process must be documented and verified. Spyware and malware target medical devices. Cybercriminals and hackers are looking for the most lucrative return on investment of time and money per attack. So, if the health device or the network are insecure and easy to hack the attackers will choose it as an "soft target" to launch attacks against.

V. Attacks on Healthcare Devices

In cyber-attacks, the primary factors to consider are integrity, confidentiality and/or accessibility in the systems. Evidence from the past century has revealed that, even though medical devices were digitalized and integrated over time, the level of security was remarkably inadequate. US FDA facts show that software errors are leading to increasing numbers of recalls of medical devices. While no one is believed to have caused death through breaching into a medical device until now, numerous researchers have also found that it could be. A team of researchers exposed attacks on implantable heart defibrillators in 2008. The group was able to extract private information from a patient using the help of a widely accessible computer program and alter the pacemaker's program to prevent service. There have been numerous studies that have shown various methods of targeting insulin pumps and pacemakers [10,11,12]. As of the month of May 2017, cybersecurity company analysts White Scope discovered a total of 8,665 documented and exposed issues discovered by four specific pacemaker programmers from various suppliers of third-party software sources [19].

VI. Structural Barrier sand Vulnerability

Many structural issues increase and complicate the security of cybersecurity risks for medical devices. Because medical devices are complicated systems, security procedures must be enforced across the network as well as across the different sheets. As an example, some aspects of the medical device can be accomplished through an internet connection that is not connected to the device. A computer such as a laptop could perform crucial tasks when utilized for medical purposes, i.e., purposes of monitoring or treatment. Security of medical systems entails the collaboration of obligations between the suppliers and users of the various components of the system. This section provides an overview of the various structural aspects that impact the vulnerability of medical systems. Additionally, such issues can be found in numerous Cyber-physical Systems (CPS) where there are numerical controls used in transportation, electricity and development, like. Change between security protection, security, and other important specifications of the device The challenge is to find a compromise between the security objectives of medical systems as well as the safety and utility of healthcare. Medical equipment that is dependent on integrated computer systems that are limited in computing power as well as storage capacity and energy consumption. The use of cryptographic functions can narrow the process down, reducing the battery's life, making appliances unusable in emergencies.

Private and unclear Software: A lot of medical devices rely on software that is free and frequently not accessible to OEMs (Original Equipment Makers). Distributors and retailers aren't always open with access to certain components of third-party software in the devices. The testing of the program is difficult. OEMs need to consider the application as a "black box" in test aspects. There are many dangers to safety, such as security flaws, or cypher malfunctions

that are mitigated when Service providers provide the software to OEMs or testing and inspection laboratories. Incomplete security updates and patching (in time) If the security flaw has been identified and the system is patched, it must receive regular security updates the software. The software must be updated with timely security updates [14]. But, it's harder to repair medical devices than it is to fix IT operating systems [15, 16]. Updates can pose security risks if they communicate in a strange way with the environment of the application or render applications inaccessible. Updates to the software must not just solve security problems within a particular application, but must also make sure that they that there are no unwanted difficulties or inconsistencies between other hardware and software on the network, such as the previously mentioned systems. If updates to software were not properly delivered it is possible for them to be used to channel harmful software into programs. Changes can alter the functions of the software. By means of an updated time-taking acceptance or an evaluation process manufacturers are required to provide them. Due to this, patches delivery can be delayed. US FDA does not permit non-healthy updates due to mandatory training processes for speeding up the release of patches. In the end, delivery and maintenance tasks aren't always simple. Hospitals, and other users of medical devices, typically depend on the vendors to provide updates, and then lose the damage claim if they themselves update or alter the software used by the equipment.

VII. Discussion

Based on our research It is pertinent to note that the cyber security requirements are standard requirements that only perform protection and preventive functions to healthcare IoT systems. They do not respond to all of the attacks and vulnerabilities. They are only efficient in defending against known threats, whereas the medical devices and sensors that makeup IoT are placed in open and uncontrolled environments with untrusted and insecure organizations. Thus, security issues and risks within healthcare facilities are more complex than those in other sectors. For instance, the information of patients is extremely private and sensitive and having access to up-to-date information is essential in healthcare occupations. With the advancement of technology security requirements for IoT systems are changing from a security-focused approach to a cyber-resiliency model that incorporates features like prevention of faults, prediction and autonomic computing, which covers all attacks and threats, whether not known or unknowable [13, 41]. In the end, security requirements that are based on a resilient approach should be taken into consideration for the healthcare IoT architecture. Cyber-resilient systems are one element of the trustworthiness requirements and also includes other security elements like security, reliability as well as privacy and safety.

It is claimed that If IoT devices can satisfy both demands of cyber resilience as well as cybersecurity, they will attain the highest level of trustworthiness and provide users with secure healthcare services that will eventually lead to the widespread adoption by the use of IoT technology. In this regard, Safavi et al. have identified six key features of cybersecurity requirements for healthcare IoT-related: confidentiality authenticity integrity, integrity and authorization accessibility as well as non-repudiation. Moreover, MacDermott et al. have argued that integrity and availability are essential security features in IoT. By contrast, Koutli et al. have suggested more security standards for each layer of the e-health IoT architecture,

including security, authentication security, confidentiality, integrity accessibility, privacy, and management of the trust. Particularly, they've examined the importance of trust between IoT nodes, which will ensure that there is a high degree of trust to recognize malicious nodes within this network. Jaiswal et al. have looked at the requirements for both cybersecurity and resilience and have emphasized the importance of trustworthiness of healthcare IoT equipment. Almohri et al. have proposed the trust model for every level of the medical IoT system that includes communication links, software hardware and platform, as well as the users [27]. Mahmoud et al. have addressed IoT security concerns, such as privacy and confidentiality, authentication, access control and management of trust. Jaigirdar et al. believed that reliable standards should be incorporated into every layer of the health IoT system. Similarly, Jaiswal et al. have noted that trustworthiness can be obtained by following all the Security specifications. Trustworthiness is actually a broad term that covers every security feature, including security privacy, maintainability, performance, reliability, survivability and security.

A significant portion of cyber resilience needs is focused on the characteristics of maintenance ability, which implies that IoT systems must be able to fix or modify malfunctions and adjust to various operational conditions. In this respect, Algarni et al., Islam et al., and Jaiswal et al. have highlighted security aspects that are related to maintaining the system [3, 27, 30]. Additionally, autonomic computing, as an aspect of maintainability is among the most important features to meet cybersecurity resilience needs. Autonomic computing or self-awareness is a key element in the self-management of IoT-connected healthcare systems. It is achieved by self-protecting, self-configuring automatic self-healing and auto-optimizing. It's surprising that most of the studies that have been conducted on IoT security within the healthcare industry have not dealt with security aspects, while safety regulations are a key element for all equipment of IoT devices, such as medical devices, sensors, and patients. But, as per NIST standards, security guidelines ensure that there are no risks of injuries, death, malfunction or the loss in the use of devices [41].

VIII. Conclusion

The healthcare industry has witnessed the rise of a variety of IoT devices and applications. These devices are responsible for sensitive and personal data like personal health information and could be targeted by cybercriminals. It is crucial to understand the aspects and the concepts of security requirements for healthcare IoT. This study looked at published research studies about the security requirements of healthcare IoT. The findings from this study will be of interest to different groups like researchers, engineers working in information technology as well as health professionals and policymakers who are concerned with IoT and healthcare technology. This study provides a reason to continue studies and create a robust healthcare system based on IoT.

IX. References

1. Vidhya K, Kumar B. (2022). The impact of Covid 19 towards insurance and its benefits to public. Mathematical Statiscian and Engineering Application ISSN 2094-0343 , 2326-9865 .Vol. 71 No. 3s , Page no 1484-1491

2. Safavi, A. M. Meer, E. Keneth Joel Melanie and Z. Shukur, "Cyber Vulnerabilities on Smart Healthcare, Review and Solutions," 2018 Cyber Resilience Conference (CRC), Putrajaya, Malaysia, 2018, pp. 1-5.
3. M. Skierka, "The governance of safety and security risks in connected healthcare," Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, 2018, pp. 1-12
4. Apurva Mohan and Douglas M. Blough, "AttributeTrust - A Framework for Evaluating Trust in Aggregated Attributes via a Reputation System", Sixth Annual Conference on Privacy, Security and Trust (PST '08), Fredericton, NB, Canada, October, 2008.
5. Ghadeer H. Cybersecurity Issues in Internet of Things and Countermeasures; Proceeding of 2018 IEEE International Conference on Industrial Internet (ICII). 2018 Oct 21-23; 2018; Seattle, Washington, United States. IEEE; pp. 195–201.
6. Kumar B. (2022). The continuous investment in artificial intelligence and its impact on ensuring customer satisfaction. Korea review of international studies, Volume 15
7. Kumar B. (2019). Factors affecting tax audit effectiveness in East Gojjam zone revenue office in Ethiopia .Think India journal , ISSN: 0971-1260 vol-22
8. Kumar B. (2020). Magnitude, determinants and effect of illegal outmigration from South Wollo Zone with special reference selected woredas. European Journal of Molecular & Clinical Medicine ISSN 2515-8260 Volume 07, Issue 10, 2020 pages 2936 to 2955
9. Kumar B. (2020). Determinants of Dividend Payout Ratio: Empirical Evidence from Ethiopian Private Banks. Palarch's Journal of Archaeology of Egypt/Egyptology 17(7). ISSN 1567-214x from page no 14823 to 14836.
10. Poyner I, Sherratt RS. Proceeding of the Living in the Internet of Things: Cybersecurity of the IoT. 2018 Mar 28-29. London, UK: Institution of Engineering and Technology (IET); 2018. Privacy and security of consumer IoT devices for the pervasive monitoring of vulnerable people; pp. 1–5.
11. Dogaru DI, Dumitrache I. Cyber security in healthcare networks; Proceeding of The 6th IEEE International Conference on E-Health and Bioengineering Conference (EHB). 2017 Jun 22-24; 2017; Sinaia, Romania. IEEE; pp. 414–417.
12. Kumar B. Getish , B. Bezabh , (2020). The Effect of Remittance on Economic Growth of Eastern African Countries. International Journal of Social Science & Management Studies. Page-13-26
13. Mengist W. , Kumar B.(2018). A Conceptual study of Micro Finance in India. International Journal of Marketing & Financial Management, Vol. 5, pp. 75-82. ISSN: 2348 -3954 (Online) ISSN: 2349 - 2546 (Print).
14. Kumar B. (2017). A critical analysis of Micro finance institutions – Impact as magical bullet to rural. Kumar,. S.L. : Excel India publishers, 2017. Vol. 1.
15. Kumar B. (2011). Special Economic Zones- A Comparative Study of Export and FDI with India. Metamorphosis- A Journal of Management Research, Vol. 2, pp. 18-28. ISSN: 09726225 and E-ISSN: 23489324.
16. Lee JD, Yoon TS, Chung SH, Cha HS. Service-Oriented Security Framework for Remote Medical Services in the Internet of Things Environment. Healthcare informatics research. 2015 Oct;21(4):271–282.

17. Jaiswal S, Gupta D. Security Requirements for Internet of Things (IoT). Proceedings. Singapore: Springer Singapore; 2017. pp. 419–427.
18. Pawan Kumar Tiwari, Mukesh Kumar Yadav, R. K. G. A. . (2022). Design Simulation and Review of Solar PV Power Forecasting Using Computing Techniques. International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(5), 18–27. https://doi.org/10.17762/ijrmee.v9i5.370
19. Kumar B. (2022). The Role and Outreach of Pradhan Mantri Jan Dhan Yojana (PMJDY) Scheme -An Financial Inclusion Programme with Special Reference to Chennam Pallipuram Region, Kerala, IJRAR May 2022, Volume 9, Issue 2
20. Kumar B. (2022). Application of blockchain technology as a support tool in economic & financial development. Manager- The British Journal of Administrative Management, ISSN:1746-1278
21. Kumar B. (2022). Deposit mobilization & branch expansion dimensions- a critical analysis with special reference to Dashen bank Ethiopia. GIS Science Journal ISSN NO : 1869-9391 VOLUME 9, ISSUE 3, 2022 Page: 175-197
22. Kumar B. (2021). Innovation in corporate cash holding & management: an empirical investigation. Empirical Economics Letters, ISSN 1681 8997
23. Kumar B. & D. Singh (2021). The impact of branch expansion dimensions on deposit mobilization with special reference Dashen bank S.C, Ethiopia. International Journal of Mechanical Engineering I ISSN: Vol. 6 P.625-636
24. Kumar B. (2021). Determinants of internet financial reporting: in the case of Ethiopian insurance and banking sector companies. Innovations , Journal article
25. Kumar B.(2020). Determinants of dividend payout ratio: empirical evidence from Ethiopian private banks. Palarch's Journal of Archaeology of Egypt/Egyptology
26. Kumar B. (2019). The effect of remittance on economic growth of eastern African countries. International Journal of Social Science & Management Studies Vol. - 6, No. – 1 Page-13-26
27. Kumar Bhupendra (2011). Special Economic Zones – a comparative study of export and FDI performance with India. Metamorphosis- A Journal of Management Research, Vol. 2, pp. 18-28
28. Pawan Kumar Tiwari, P. S. . (2022). Numerical Simulation of Optimized Placement of Distibuted Generators in Standard Radial Distribution System Using Improved Computations. International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(5), 10–17. https://doi.org/10.17762/ijrmee.v9i5.369