International Journal of Engineering Sciences & Emerging Technologies, Oct. 2023.
ISSN: 22316604 Volume 11, Issue 2, pp: 359-367 ©IJESET

INTERNET OF THINGS (IOT) APPLICATIONS AND CHALLENGES: A REVIEW

Satendra Kumar, Kanchan, Amit Kumar, Prachi Agarwal, Himanshu Maurya

Department of Computer Science & Engineering,
Moradabad Institute of Technology (U.P), India
satender04cs41@gmail.com,kanchansinghcs@gmail.com, amitakg84@gmail.com,
reachtoprachi@gmail.com,mauryahimanshu987@gmail.com

ABSTRACT

The idea behind the Internet of Things (IoT) is to connect various gadgets to the internet and one another to communicate several bits of information and data. The Internet of Things is revolutionizing many aspects of life, including how we drive, shop, and even acquire electricity for our houses. All around us, there are sophisticated electronics and sensors embedded. How we use these tools and how they exchange data and knowledge. An overview of various platforms, architectures, applications, and problems is provided in this study.

KEYWORDS: *Digital Internet-of-Things (IoT), IoT applications, personal health, IoT platforms, sensors*

1. INTRODUCTION

The Internet of Things (IoT), a ground-breaking paradigm, has emerged, enabling common objects to be connected to the internet and collect and exchange data. This review article provides a thorough analysis of IoT and the many sectors it serves. By closely examining its fundamental components, like connected devices and communication protocols, we can fully comprehend the underlying structure of IoT systems.

The Internet of Things (IoT) is a network of physically addressable devices with varying degrees of computing, sensing, and actuation capabilities that may collaborate and communicate with one another utilizing the Internet as their common platform [1]. The Internet is the name of the communication system that links people to information. The basic goal of the Internet of Things is to link things and people at any time or location via any network, method, or service. IoT will enable common gadgets to connect and access the internet in order to achieve a variety of goals. As of this writing, only 0.6% of potential IoT devices are thought to be connected [2]. But it's predicted that by 2020, there will be more than 50 billion internet-connected devices. Fig. 1 illustrates how the Internet of Things (IoT) "connected" various functions of devices and a network [3], whereas the Internet has evolved into a network of many devices rather than just a network of computers. The ability to transmit information online is now present in various gadgets, such as smartphones, cars, industrial systems, cameras, toys, structures, home appliances, and numerous other things. Regardless of their size, these devices can carry out intelligent reorganizations, tracking, placement, control, real-time monitoring, and process control and capacities. There have been a lot more devices in recent years that can connect to the Internet. Even if the popularity of wearable technology (watches, headsets, etc.) and the rise of smartphones have had the greatest commercial impacts on the consumer electronics industry, Only a small portion of a bigger trend toward the blending of the physical and digital worlds is linking individuals. In light of everything said above, it is projected that the Internet of Things (IoT) will continue to expand in terms of the variety of devices and capabilities it can support. It is difficult to define the IoT's increasing bounds because of the vagueness of the word "Things" [4]. While commercial success is still a long way off, For

corporations and academics, the Internet of Things (IoT) continues to present what seems like an inexhaustible supply of potential. The paper covers the many IoT domains in light of this applications that could be used as well as the corresponding research difficulties.

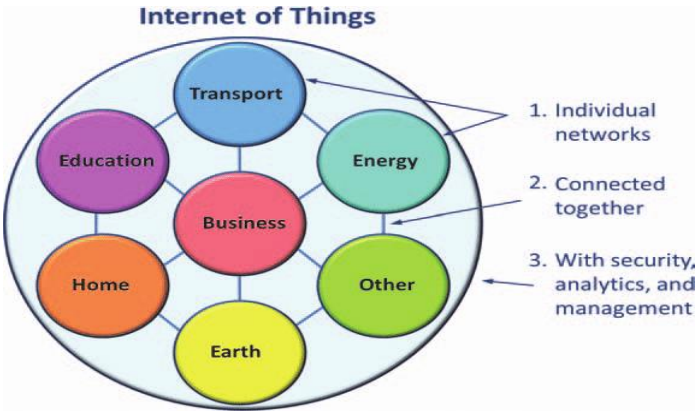

Figure 1. IoT can be viewed as a Network of Networks [3].

2. Related Work and Research Directions

Numerous research papers and survey articles on IoT have been published. Reference [5]'s writers looked at the security of the eight systems that make up the key IoT architecture. For each structure, we outline the suggested architecture, the principles of creating outsider cunning software, the suitable hardware, and the security features. Reference [6] investigated the IoT holistically by referencing a variety of IoT designs, demonstrating potential, IoT components, related enhancements, standard application conventions, fundamental issues, and open research concerns in the IoT field. Reference [7] presented different corporate IoT topologies and provided a comparative analysis based on the methods employed, the conventions supported, industrial use, equipment requirements, and application development. The writers of [8] looked at four different angles on the difficulties with IoT security and protection. They begin by highlighting the difficulties with IoT device security implementation (such as battery life and processing power) and suggested solutions (such as lightweight encryption conspire for installed frameworks). The descriptions of IoT attacks are also condensed (physical, remote, close, etc.). Thirdly, they focus on the components and plans created and implemented for verification and approval purposes. The security issues at the various layers (physical, organizational, and so forth) are then separated. The existing Web of Things IETF models are briefly summarised in [9]. The definition of IoT, the techniques by which it delegated numerous developments, relating its engineering, qualities, and applications, IoT relevant concept, and what the obstacles for IoT are in the future were quickly examined by creators in [6] [10] provides a comprehensive overview of the IoT along with an analysis of the current designs, supporting technologies, applications, and research challenges for the IoT. From the need for vehicle information and its uses to empowering breakthroughs, challenges, and extraordinary prospects, the paper in [12] summarises the best of the best in linked vehicles. In [13], a thorough review of the IoT's framework engineering, empowering developments, security and protection difficulties, and synchronization of haze/edge registering and IoT, as well as applications, are covered. The interplay between IoT and CPS, both of which demand a lot of work to realise an understanding of the cyber-physical environment, is the focus of this work. The paper in [11] provides an overview of the Industrial Internet, focusing on its architecture, supporting technologies, applications, and current challenges.

3. IoT Platform Architecture

To handle a network as large as the Internet of Things, which is anticipated to have more than 25 billion connected devices by 2020 [14], a new open architecture that may serve the existing network applications while addressing numerous security and Quality of Service (QoS) issues is required. By 2020, there will likely be more than 25 billion linked devices, according to estimates [15]. If a sufficient

amount of privacy assurance is not offered, it is unlikely that IoT will be broadly adopted [17]. Data protection and user privacy are thus two of the main IoT difficulties [18]. A number of multi-layered security architectures are advised for the ongoing development of IoT. Three key levels were used to define IoT architecture in [19], however, a four-key level design was given in [20]. The Internet and Telecommunication Management Network technologies based on TCP/IP and TMN were combined into a five-layered design in [21].
A six-layered architecture built on the network hierarchical structure was also proposed which is similar to this. It is often divided into six levels, as seen in Fig. 2.
Each of the six IoT layers is described below:

3.1. Coding Layer

Coding serves as the IoT's structural base and identifies things of interest. Since each object in this layer has a distinct ID.

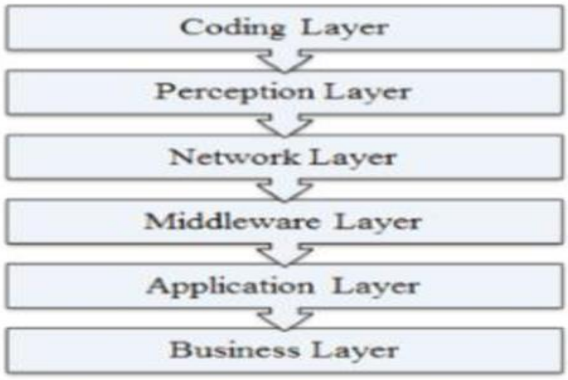

Figure 2. Six-Layered Architecture of IoT

3.2. Perception Layer

Each thing must be given a distinct meaning by the IoT device layer. It is composed of information sensors that can identify an object's position, velocity, temperature, humidity, and other attributes. RFID tags, IR sensors, and other sensor networks are examples of data sensors. Through sensor systems attached to the objects, this layer gathers important information about them, converts it into digital signals, and transmits the signals to higher layers, digital signals for further processing at the network layer.

3.3. Network Layer

The purpose of this layer is to accept useful data from the perception layer as digital signals and transmit it to the processing units of the middleware layer utilising a range of communication channels and protocols, including as WiFi, Bluetooth, WiMaX, Zigbee, GSM, and 3G.

3.4. Mid-Level Layer

The data that the sensor devices transmit is processed at this layer [2]. It is designed with cloud computing and ubiquitous computing features, which allow for immediate access to the database and the storage of any required data there. The results of the information processing are then used to trigger a completely automated action. Utilizing some sophisticated processing machinery, the information is processed.

3.5. Application Layer

Based on the data that has been processed, this layer functionalizes IoT applications for several sectors. Applications contribute to the Internet of Things development, therefore this layer is essential for the network's rapid expansion. The Internet of Things has several uses, including smart planets, intelligent cars, and smart cities.

3.6. Business layer

This layer is in charge of managing IoT services and applications and doing any related research. Numerous business models are produced for practical firm strategy [1].

4. TECHNOLOGIES

The creation of a system for everywhere computing, in which digital objects are capable of individually identifying themselves, reasoning, and interacting and observing other entities to determine which automated actions are based, calls for the fusion of Interoperability across multiple technologies is the sole thing that enables the development of new and efficient technologies that enable object identification and communication. This section discusses the key technologies that can aid in the IoT's development in general.

4.1. RFID, or radio frequency identification

RFID is the primary method for making things individually identifiable. It can be used in any product because of its small size and low cost [19]. Depending on the application, it is a transmitter microchip that resembles an adhesive sticker and can either be active or passive. Active tags are always on and continuously send out data signals since they are powered by a battery, whereas passive tags only activate when they are triggered. Despite being more expensive than passive tags, active tags are much more useful [2]. The RFID system is made up of readers and associated RFID tags that, when activated by the generation of any appropriate signal, convey data about the object, including its identification, position, and other specifics. The processors receive the radio frequencies used to send the produced object-related data signals and use them to analyse the data.

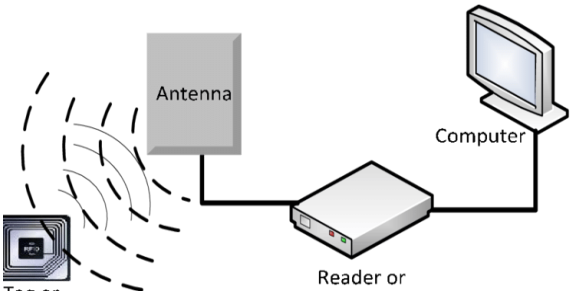

Figure 3. RFID

RFID frequencies are separated into four distinct frequency bands [18], which are listed below, depending on the intended use:

1. (135 KHz or above) quite infrequent
2. (1.35.6 MHz) High Frequency
3. Ultra-High Frequency (862–928 MHz)

(2.4G, 5.80) Wireless Wavelength Bar Code is a different identifying technology that serves a similar purpose to RFID, however it is less efficient than RFID for a variety of reasons. Instead of requiring the reader to be physically in its line of sight like RFID, which employs radio technology, bar codes are optical technologies that require the reader to be positioned in front of them in order to work. In addition, unlike bar codes, an RFID can act as an actuator to initiate a variety of actions, including changes.

4.2 WSN, or wireless sensor network

A WSN is a wireless sensor network with many hops that is bi-directional and composed of nodes dispersed throughout a sensor field. Each of these nodes is connected to a sensor that can gather information about an object, such as its climate, moist, rapidity, etc., and transmit it to the equipment for processing. Communication between the sensing nodes involves several hops. The communication,

actuation, and sensing components of the sensors are an antenna, a microcontroller, and an interface circuit, respectively making each sensor a transceiver. Each sensor is powered independently, either by a battery or another energy-harvesting system [2] proposed a second memory unit for data storage, albeit it might alternatively be a component of the sensing node. An illustration of a sensing node can be found below:
Mobile Sensors When network technology and RFID technology are integrated, the potential for even more smart devices has been addressed by a number of solutions. The Wireless Identification Sensing Platform (WISP) from Intel Research Labs is an illustration of a remedy. A passive wireless sensor network called WISP has built-in sensors for light, temperature, and other things. WSNs have a considerably broader range and peer-to-peer communication, but RFID Sensor Networks have a small range and asymmetric communication. Both WSN and RFID Sensor Networks offer advantages. The majority of WSNs are also constructed in accordance with the IEEE 802.15.4 standard, which outlines the Physical and MAC layers of Low-Rate Wireless Personal Area Networks. This protocol enables the transmission of IPv6 packets over networks with constrained processing power. Another choice for end-to-end routing systems is the ROLL routing standard.

4.3. Cloud Computing

The cloud seems to be the only technology capable of effectively analysing and storing all the data, with millions of devices predicted by 2020 [14]. To enable resource sharing that is accessible at any time and from any location, a cloud platform aggregates several servers. Cloud computing, which unifies servers, accelerates data processing, analyses priceless sensor data, and even provides enough storage, is a crucial component of the Internet of Things. This technology's full potential is still unrealized. Since cloud computing will be the only source of data for IoT, research is being done to determine how cloud computing's interface with smart devices—which may use millions of sensors—can have huge advantages and enable IoT to flourish on a very large scale.

4.4. Nanotechnologies

This technology helps linked objects become better and smaller. It can lower the consumption of a system by simplifying the development of nanometre-scale devices that can serve as a sensor and an actuator just like a typical device. Such a nano-device is made of nanomaterial, and the Internet of Nano-Things network it forms establishes a new paradigm for networking.
Technologies for Micro-Electro-Mechanical Systems (MEMS) MEMS, which are already commercially accessible in the form of transducers, accelerometers, and other devices, can be used for a range of functions, including sensing and actuating when mechanical and electrical components are integrated. The IoT's communication system is enhanced by MEMS and Nanotechnologies, which also offer other advantages including smaller sensors and actuators, integrated ubiquitous computing devices, and a larger frequency range.

5. IoT Applications

1. Smart Home: Networked appliances and devices are made possible by IoT to create smart homes. Users can remotely operate and keep an eye on security systems, lighting, temperature, entertainment systems, and other home appliances.
2. The Internet of Things has a significant impact on the healthcare industry. It makes it possible for patients with chronic conditions to have real-time health monitoring, wearable health monitoring devices, remote patient monitoring, and smart medication management systems.
3. Industrial Automation: The Internet of Things is enabling automated manufacturing, which is revolutionizing the industrial sector. IoT sensors and devices track and improve manufacturing operations, estimate maintenance needs, manage stocks, and boost overall efficiency.
4. Smart Cities: IoT is crucial to the development of sustainable and intelligent cities. It includes waste management choices, environmental monitoring, smart traffic management systems, smart street lighting, and infrastructure optimization for effective urban life.

5. Agriculture: IoT technology is revolutionizing agriculture by enabling precision agricultural techniques. IoT sensors may be used by farmers to keep an eye on soil moisture, temperature, and crop health, which will help them enhance irrigation, manage pests, and increase agricultural productivity.
6. Energy Management: IoT enables the management and optimization of energy consumption. Smart meters, energy monitoring systems, and smart grids enable better energy monitoring, control, and optimization, which raises productivity and lowers costs.
7. Transportation and Logistics: Effective fleet management, route optimization, real-time shipment tracking, and vehicle monitoring are all made possible by IoT. It enhances the efficiency of the entire supply chain, uses less fuel, and enables better logistical planning.
8. Monitoring of the environment: IoT sensors and devices are utilized to keep track on environmental elements like wildlife, water management, and air quality. The utilization of this data facilitates making well-informed decisions for resource management and environmental preservation.
9. Retail and Supply Chain: A few IoT applications in the retail industry include smart shelves, inventory management, consumer tracking, and customized shopping experiences. IoT enables the supply chain to do real-time tracking, preventive maintenance, and efficient inventory management.
10. Safety and Security: The Internet of Things (IoT) enhances safety and security through applications including smart surveillance systems, smart locks, fire detection systems, and emergency response systems. Remote control, monitoring, and alerting in real-time are all made feasible.

6. IoT CHALLENGES

Although the Internet of Things (IoT) has many advantages, there are also several issues that need to be fixed before it can be successfully used and widely adopted. Here are a few of the main challenges the Internet of Things poses:

1. Security and privacy: IoT devices are susceptible to cyber security attacks due to their extensive use and connectivity. Strong security measures must be in place to prevent data breaches, unauthorized access, and privacy violations. In addition, the collection and storage of massive amounts of personal data by IoT devices raises concerns about privacy protection.

2. Interoperability and Standards: A wide range of products from numerous suppliers are used in the Internet of Things (IoT). Effective device and system integration and communication may be hampered by interoperability problems and a lack of standardized protocols. Common standards and frameworks must be defined in order for the various IoT components to work together and be interoperable with one another.

3. Scalability and Network Management: As the number of connected devices increases exponentially, managing the scalability and network infrastructure of IoT systems becomes challenging. To control network congestion, handle growing data volumes, and ensure dependable connectivity, solid network management strategies and infrastructure upgrades are required.

4. The massive amounts of data that the Internet of Things (IoT) creates must be efficiently managed, stored, processed, and assessed. Managing real-time data streams, ensuring data quality, and getting usable insights from the data collected are all very challenging tasks. Adequate data management and analytics strategies must be used in order to maximise the value of IoT data.

5. Power Consumption and Energy Efficiency: Because a lot of Internet of Things (IoT) devices are battery-powered, lowering power consumption is crucial to extending their lifespan. Energy-efficient designs, low-power communication protocols, and effective power management techniques must be used to increase the energy efficiency of IoT devices and systems.

6. Ethical and Social Implications: The Internet of Things (IoT), which has ethical and social implications, raises questions about data ownership, consent, and the risk of surveillance. It is crucial to address issues like data ownership, transparency, accountability, and the formation of ethical frameworks in order to ensure responsible and trustworthy IoT deployments.

7. Cost and Return on Investment: Implementing IoT solutions can be costly in the beginning because it requires setting up infrastructure, deploying devices, and installing data management programs. Businesses must ensure a clear understanding of the return on investment (ROI) and long-term viability in order to defend their IoT investments and benefit from the installed systems.

8. Regulatory and Legal Considerations: Regulations governing data protection, privacy, and industry-specific regulations are among the criteria that IoT deployments must abide with. Implementing IoT successfully necessitates negotiating the legal system, upholding compliance, and addressing potential liability issues.

To solve these problems, cooperation between a numbers of parties is required, including technology providers, policymakers, standards organisations, and end users. By proactively addressing these challenges, the full potential of IoT may be realised while ensuring a secure, interoperable, and socially acceptable IoT ecosystem.

7. CONCLUSION

In conclusion, the Internet of Things (IoT) has emerged as a paradigm-shifting technology with a wide range of applications. This article provides a thorough review of IoT and its uses, highlighting how it has the potential to revolutionize sectors like healthcare, manufacturing, smart cities, agriculture, retail, logistics, and environmental monitoring.

The main components of IoT systems that were the subject of the review were linked devices, communication protocols, and data management frameworks. It underscored the importance of robust security measures, data privacy considerations, and interoperability standards to enable the successful integration and usage of IoT technologies.

IoT has the ability to enhance decision-making, increase efficiency, make the greatest use of resources, and provide individualized experiences, as was made obvious by looking at how it is used in a variety of industries. Precision agricultural techniques, industrial predictive maintenance, smart city infrastructure, and remote hospital monitoring are just a few of the industries in which the Internet of Things is revolutionizing and creating new opportunities.

However, the review also mentioned the drawbacks of IoT, including security threats, interoperability issues, scalability problems, and ethical concerns. It stressed the significance of resolving these issues through interdisciplinary collaboration, standardization initiatives, and regulatory frameworks in order to ensure the responsible and sustainable spread of IoT.

Future possibilities for IoT are promising. The potential and capabilities of IoT applications will increase as a result of technological developments in fields like edge computing, AI, and 5G networks. By utilizing the revolutionary potential of IoT and proactively addressing the issues, we can set the stage for a connected, intelligent, and productive future.

Finally, this evaluation is a helpful resource for decision-makers, professionals, and academics who want to understand the variety and complexity of IoT applications. By using the knowledge gained from this research, stakeholders may make informed decisions, encourage innovation, and realize the full potential of IoT for the benefit of society.

REFERENCES

[1] Miraz, M. H., Ali, M., Excell, P. S., & Picking, R. (2015). A review on Internet of Things (IoT), Internet of everything (IoE) and Internet of nano things (IoNT). *2015 Internet Technologies and Applications (ITA)*, 219-224.

[2] Ryan, P. J., & Watson, R. B. (2017). Research challenges for the internet of things: what role can or play?. Systems, 5(1), 24.

[3] Miraz, M. H., Ali, M., & Peter, S. (2018). Excell, and Richard Picking,". *Internet of Nano-things, Things and Everything: Future Growth Trends,"(to be published) Future Internet*.
[4] Borgia, E., Gomes, D. G., Lagesse, B., Lea, R., & Puccinelli, D. (2016). Special issue on "Internet of Things: Research challenges and Solutions". *Computer Communications*, *89*, 1-4.
[5] Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, *38*, 8-27.
[6] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, *17*(4), 2347-2376.
[7] Derhamy, H., Eliasson, J., Delsing, J., & Priller, P. (2015, September). A survey of commercial frameworks for the internet of things. In *2015 ieee 20th conference on emerging technologies & factory automation (etfa)* (pp. 1-8). IEEE.
[8] Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of things Journal*, *4*(5), 1250-1258..
[9] Sheng, Z., Yang, S., Yu, Y., Vasilakos, A. V., McCann, J. A., & Leung, K. K. (2013). A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities. *IEEE wireless communications*, *20*(6), 91-98.
[10] Patel, K. K., Patel, S. M., & Scholar, P. (2016). Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. *International journal of engineering science and computing*, *6*(5).
[11] Siegel, J. E., Erb, D. C., & Sarma, S. E. (2017). A survey of the connected vehicle landscape—Architectures, enabling technologies, applications, and development areas. *IEEE Transactions on Intelligent Transportation Systems*, *19*(8), 2391-2406.
[12] Vögler, M., Schleicher, J. M., Inzinger, C., & Dustdar, S. (2015, June). DIANE-dynamic IoT application deployment. In *2015 IEEE International Conference on Mobile Services* (pp. 298-305). IEEE.
[13] Johnson, D., & Ketel, M. (2019). IoT: application protocols and security. *International Journal of Computer Network and Information Security*, *11*(4), 1.
[14] Khanna, A., & Kaur, S. (2020). Internet of things (IoT), applications and challenges: a comprehensive review. *Wireless Personal Communications*, *114*, 1687-1762.
[15] Kotha, H. D., & Gupta, V. M. (2018). IoT application: a survey. *Int. J. Eng. Technol*, *7*(2.7), 891-896.
[16] Chen, S., Xu, H., Liu, D., Hu, B., & Wang, H. (2014). A vision of IoT: Applications, challenges, and opportunities with china perspective. *IEEE Internet of Things journal*, *1*(4), 349-359.
[17] Zeng, X., Garg, S. K., Strazdins, P., Jayaraman, P. P., Georgakopoulos, D., & Ranjan, R. (2017). IOTSim: A simulator for analysing IoT applications. *Journal of Systems Architecture*, *72*, 93-107.
[18] Ahamed, J., & Rajan, A. V. (2016, December). Internet of Things (IoT): Application systems and security vulnerabilities. In *2016 5th International conference on electronic devices, systems and applications (ICEDSA)* (pp. 1-5). IEEE.
[19] Singh, R. P., Javaid, M., Haleem, A., & Suman, R. (2020). Internet of things (IoT) applications to fight against COVID-19 pandemic. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, *14*(4), 521-524.

Authors

Satendra Kumar is an Assistant Professor in the Department of Computer Science & Engineering, Moradabad Institute of Technology, Moradabad. He completed his Ph.D. from Gurukula Kangri (Deemed to be University) , Haridwar, Uttarakhand in 2020. He received his MTech degree in Computer Engineering from YMCA University of Science and Technology Faridabad in 2012. He pursued his BTech degree from MJPRU Bareilly. He has published more than 20 research papers in various international journals and conferences. He has more than 10 years teaching and research experience. His research interests include software engineering, software product line and soft computing techniques.

Kanchan Rani is an Assistant Professor in the Department of Computer Science & Engineering, Moradabad Institute of Technology, Moradabad. She completed her MTech degree in Computer Science from Banasthali Vidyapith Jaipur in 2011. She pursued her BTech degree from AKTU Lucknow. She her published more than 18 research papers in various international journals and conferences. She has more than

16 years teaching experience. Her research interests include Artificial Intelligence, Machine Learning, software engineering and soft computing techniques.

Amit Kumar is an Assistant Professor in the Department of Computer Science & Engineering, Moradabad Institute of Technology, Moradabad. He received his MTech degree in Computer Science from Uttarakhand Technical University Dehradun in 2013. He pursued his BTech degree from Ajay Kumar Garg Engineering Coleege, Ghaziabad . He has published more than 7 research papers in various international journals and conferences. He has more than 14 years teaching experience. His research interests include Machine Learning, Deep Learning techniques , Big data & Haddoop.

Prachi Agarwal is an Assistant Professor in the Department of Computer Science & Engineering, Moradabad Institute of Technology, Moradabad. She completed her MTech degree in Computer Science from IFTM University in 2013. She pursued her BTech degree from GBTU Lucknow. She her published more than 15 research papers in various international journals and conferences. She has more than 11 years teaching experience. Her research interests include Machine Learning, web development and image processing**.**

Himanshu Maurya is pursuing B.Tech. in Computer Science & Engineering from Moradabad Institute of Technology, Moradabad. Areas of interest include Machine Learning.