İSTANBUL UNIVERSITY CERRAHPAŞA

ORIGINAL ARTICLE
Electrica 2023; 23(2): 318-328

Understanding of Network Resiliency in Communication Networks with its Integration in Internet of Things - A Survey

Shalini Sharma, Bhupendra Kumar Pathak, Rajiv Kumar

Department of Electronics and Communication, Jaypee University of Information Technology, Solan, Himachal Pradesh, India

Cite this article as: S. Sharma, B. K. Pathak and R. Kumar, "Understanding of network resiliency in communication networks with its integration in internet of things - A survey" *Electrica*, 23(2), 318-328, 2023.

ABSTRACT

Modern life is completely dependent on Internet, and as a result, network disruption has become extremely severe. It has been recognized that communication networks are not that much resilient and survivable as they need to be. Today the ongoing trend is to increase the number of services in only one communication network. All these services are distinct in their own manner as some needs low resilience requirements, whereas some of them require higher resilience. In order to fulfill these requirements, frameworks with better cost efficiency are required and these have been proposed in the literature. The work in this study provides a survey on resilience differentiation in communication networks. Along with the survey, some future challenges are also provided at the end.

***Index Terms*—**Resiliency, internet of things, availability, scalability, fault tolerance

I. RESILIENCY IN COMMUNICATION NETWORKS

A. Introduction

Networks have become a major part of various routine operations related to businesses and the economy worldwide. Internet, a part of network, is used by consumers to access distinct kinds of information, obtain products and services, and communicate with each other. Different kinds of users use different applications of Internet for satisfying their needs. Thus, the Internet can be considered the critical infrastructure on which our day-to-day activities are dependent. With the advancements in network systems, requirements of various radio access network architectures in 5G system is the demand of today's world [1].

This increase in the dependencies, however, makes the networks more vulnerable to communication-related problems and results in problem. It is continuously increasing the chances of disruption as a result making communication networks an easy and alluring target for cyber criminals. Various methods have been discussed in literature to handle problems like visible line communication by integrating it with radio frequency (WiFi) to provide quality of service to the users [2].

The resiliency of communication networks is an important aspect of network engineering. Due to the Internet protocol in networking, providing resilience characteristics like continuity and availability in the same network has become an attention-seeker topic. This study focuses on the resiliency to provide quality of services to both wireless sensor networks and IoT. The study tries to relate the resiliency in WSN with IoT networks to replace WSN with IoT. Earlier, each network was designed to offer only one kind of service either data or voice resulting in the requirement of only one level of resilience per network. One reason for the advancement in resilience differentiation is increase in the competition between various service providers and network operators to provide cost-effective services.

It can be considered that requirement of resilience not only depends on the application service but also on how the service is used by the user. So, it can be concluded that a similar kind of service can have distinct requirements as per the customer/client [3].

Resilience disciplines can be easily understood with the given Fig. 1.

Corresponding author:
Shalini Sharma

E-mail: shalinisharma5419@gmail.com

Received: July 31, 2022

Accepted: November 6, 2022

Publication Date: March 30, 2023

DOI: 10.5152/electrica.2023.22126

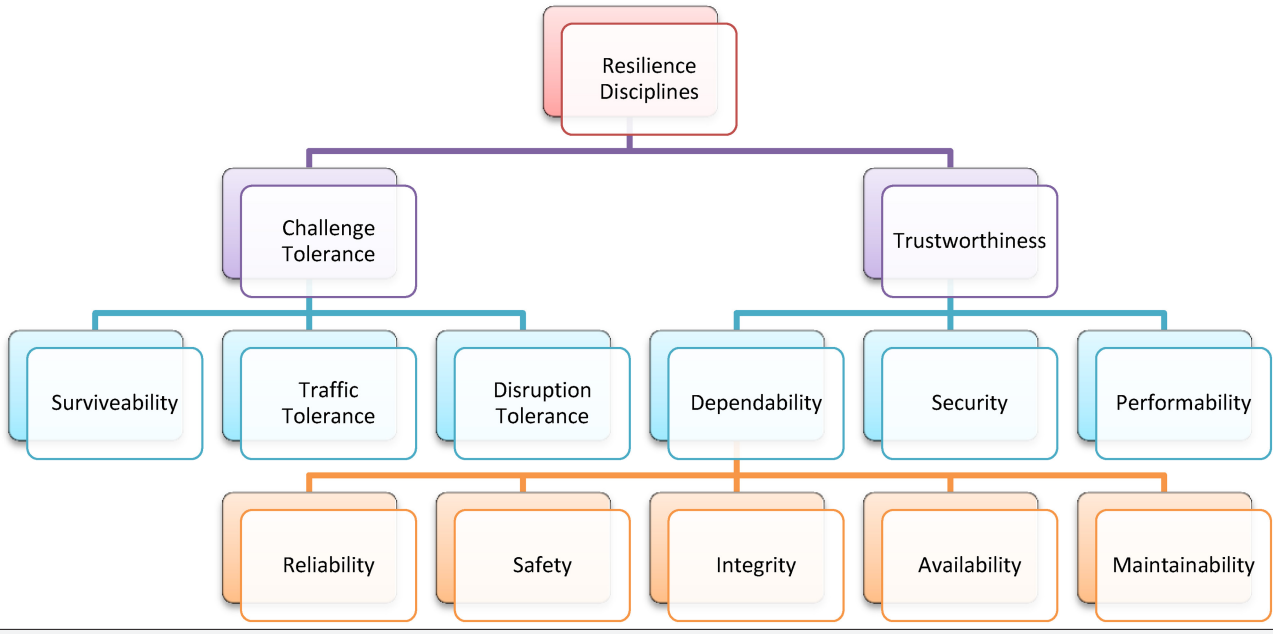

Fig. 1. Resilience discipline division.

B. Recovery in Networks

In today's networks, a large amount of data is being transmitted and many users depend on them for fulfilling their needs. In such cases, there should be a provision of tolerating the faults. The ultimate goal to achieve this is to make network more resilient and dependable so that it can automatically provide solutions to the failures like errors, link cuts, etc., by redirecting the traffic from the failed node to the other node. The recovery methods are connected not only to the connectivity but also to the Quality of Service (QoS) factors. These factors vary from layer to layer.

A brief introduction is provided here to achieve the following goals:

1) Introducing the major recovery methods and
2) Showing how different recovery methods are different in architectural sense and generating quality results.

There are few terms that need to be understood before discussing the recovery methods.

The routes on which traffic is carried out before the occurrence of fault are called primary/normal paths. In case a failure occurs, then, data are moved on to another path called recovery/backup path.

- Fault detection,
- Fault localization, and
- Fault notification

1) Classification of Recovery Methods

A large variety of recovery methods can be found in literature. Classification of recovery procedures can be done based on five standards which are given below:

1) Basis of the layer in which recovery works,
2) Basis of the path setup,
3) Basis of the intensity of resources usage,
4) Basis of the scope of a particular recovery procedure, and
5) Basis of the domain.

Standard 1 is explained in [4] and standard 2 is covered in [5].

Distinct methods and how they affect the quality of the services are tabulated in Table I.

2) Recovery-Related Quality Features

The client to whom services are provided is interested in various types of features which can be obtained either in short duration of time or long duration of time. Those are termed as the *quality of resilience*. Another type of features includes *operational-related features* in which operators require the provisioning of a particular service in the network. Thus, the features must pass on two factors; one, by meeting the clients' requirements and the other by providing profitable support to the network operator.

1) *Features Related to Quality of Resilience*

It frameworks the features that affect the quality of services needed by the users related to resilience. These features can be divided into two parts. First one is related to the reliability attributes and another is related to recovery features.

a) Reliability Attributes

Various reliability attributes can be defined as follows:

i) **Continuity:** It can be defined as the period of time during which any service is continuously working without any interruption due to the occurrence of failure. To measure continuity, the measures used are mean time to failure.
ii) **Availability:** It is another common attribute when considering the resilience of any communication network. Availability can be defined in various ways. Instantaneous availability A(t) can be defined as "what is the probability of any item in upstate at a particular instant of time" [11]. Steady state availability, A, can be explained as "what is the probability of searching any item at that instant of time when service is required by the user [12]. It can be applied in case of IP networks [13] and used to construct service-level agreements.

TABLE I. DIFFERENT METHODS AND THEIR INFLUENCE ON QUALITY

Methods	Explanation
1+1 global protection [3]	Data are transmitted simultaneously on both primary and backup path. The last node detects only one signal. In some cases, reverse backup path is used to instantly switch the data to the recovery path so smoothly that it starts with the node which finds out about the failure.
Dedicated 1+1 local protection [6]	Only faulty node is pass round, commonly known as APS in SONET systems. It ensures fast switching.
Dedicated 1:1 local protection [3]	Data are transmitted only on the original path before any failure occurs. Recovery methods need to be prepared in case any link suffers from failure.
Shared M:N local protection [3]	Both original and backup links are established before any failure occurs. In case, if more faulty links are there in comparison to backup links, then some data are lost. Frequently used method is 1:N where N-working path.
Shared M:N global protection [7]	Unlike shared M:N global protection, it pass round the whole path and also involves the egress and ingress nodes .
Shared backup path protection [3]	It shares the backup paths but it is not necessary to have common egress and ingress nodes, making the sharing of resources partial unlike shared M:N shared path protection.
Global restoration with re-provisioning [3]	Recovery of path is done after the occurrence of failure. Ingress nodes start establishing the path as soon as the fault notification occurs by using some signaling methods. It takes more recovery time as compared to shared protection methods.
Global restoration with pre-signaled recovery bandwidth reservation [3]	Unlike global restoration with re-provisioning, it retains the bandwidth of recovery path before the occurrence of any failure. But for the retention of recovery path after the failure, other signaling protocols are being used.
Flooding [8, 9]	It is a connection-oriented restoration method where the overall view of the network is not cleared to the nodes present there.
P-cycle scheme for MPLS networks fault recovery to protect LSPs and meet QoS protection parameters [10].	P-cycle for local shared protection in MLPS networks.

Unavailability can be expressed in notion of availability as

$$U \propto 1 - A \tag{1}$$

iii) **Downtime:** Downtime is a measure of the period of time during which service is inaccessible to the user because of the failure in the network. There is a direct relation of availability with mean up time and mean down time that is given below [14]

$$\text{Availability} = \frac{\text{MUT}}{\text{MUT} + \text{MDT}} \tag{2}$$

TABLE II. QOS AND TRAFFIC PARAMETERS FOR ATM

	Parameters Related to Traffic			Parameters Related to QoS		
Service Categories	**MBS**	**PCR**	**SCR**	**CLR**	**CTD**	**CDV**
CBR	N/A	Yes	N/A	Yes	Yes	Yes
Nrt-VBR	Yes	Yes	Yes	Yes	Yes	No
Rt-VBR	Yes	Yes	Yes	Yes	Yes	Yes
UBR	No	Yes	No	No	No	No

CBR, Constant Bit Rate; Nrt-VBR- Non-Real Time Variable Bit Rate, Rt-VBR- Real Time Variable Bit Rate; UBR, Unspecified Bit Rate; MBS- Maximum Burst Size; PCR, Peak Cell Rate; SCR, Sustained Cell Rate; CLR, Cell Loss Rate; CTD, Cell Transfer Delay; CDV, Cell Delay Variation

b) Recovery-Related Features

Given below are the five types of most commonly used recovery features:

1) Effect on traffic,
2) Recovery path quality,

Distinct quality of service parameters and traffic parameters for Asynchronous Transfer Mode (ATM) are given below in Table II [15].

1) Preemption,
2) Coverage in case of failure, and
3) Resilience related to multiple failures.

Fig. 2 and Fig. 3 are determining the quality of resilience features in terms of reliability attributes and recovery features, respectively.

2) *Feature related to operations*

Some of the basic parameters that need to be understood while taking operation-related features into account are mentioned below:

1) Recovery cost,
2) Scalability,

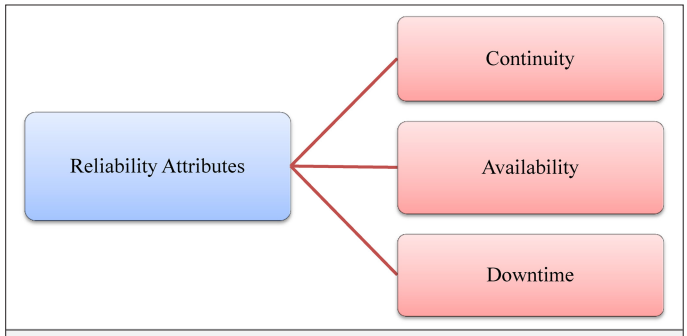

Fig. 2. Quality of resilience features: reliability attributes.

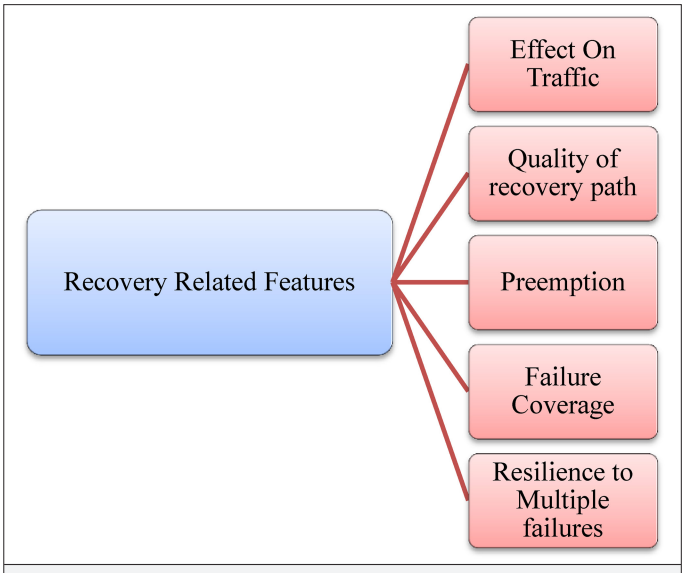

Fig. 3. Quality of resilience features: recovery-related features.

3) State overhead,
4) Flexibility, and
5) Signaling requirement.

Operational features for quality of resilience are shown in Fig. 4.

II. RESILIENCY IN IOT

A. Introduction

The latest trends in Internet have enabled the things around us to be interrelated with each other. Iot can be defined as a network connected with things that are further connected wirelessly with smart sensors. Currently, IoT can be considered to be in its initial state; still, many developments are to be done in integrating the objects with the sensors in cloud computing.

The concept of IoT was initially proposed in 1999 by Kevin Aston who stated that IoT is a uniquely identified object with Radio Frequency Identification (RFID).

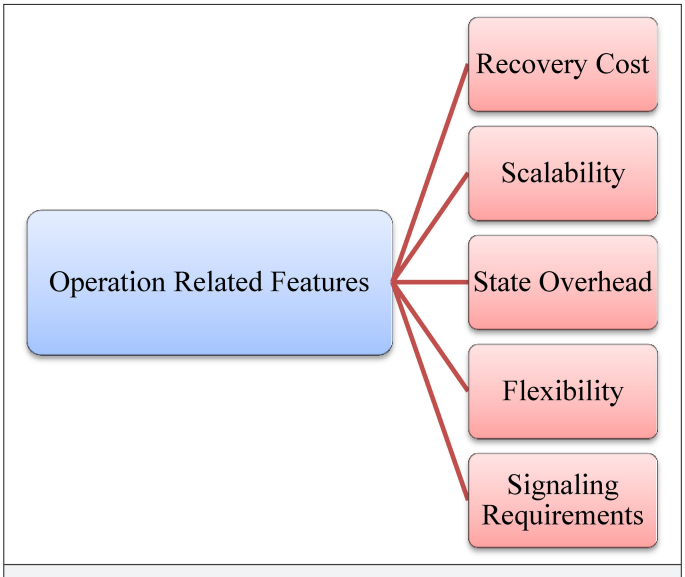

Fig. 4. Parameters related to operational-related features.

TABLE III. SUMMARY OF IOT STANDARDS

Technology	Standard
RFID Technology	ISO 11785 RFID Air Interface Protocol
	ISO 14443/15693 RFID Contactless Smart Card
	ISO 18000-2 Frequencies below 135 kHz
	ISO 18000-4 For 2.45 GHz
Communication	IEEE 802.11- WLAN
	IEEE 802.15.4- Zigbee IEEE 802.15.1- Bluetooth
	IPv6 3G/4G
Quality of Service	ITU-T

IoT, internet of things.

An IoT model consists of various performers like operators, developers, etc. Its applications can be seen in almost each field including healthcare, smart cities, smart agriculture, Industries, cyber security, and a lot more. It can be considered the next-generation model to interconnect people with devices and enable them to perform functions without the intervention of humans. Its success would need a merging of various distinct infrastructures for providing communication which further leads to the designing of smart gateways in order to connect the IoT devices to the Internet.

1) Standards

The insufficiency of standards can lower the diligence of IoT. In the previous years, a large number of technical standards by many organizations have evolved ensuring the success of IoT in each field. It includes 1) designing the architecture, 2) designing policies, 3) making sure of the privacy of users and security of networks, 4) creating standards, and 5) exploring new technologies.

Thus, it is mandatory to emphasize the significance of standards for development in the field of IoT. Thus, maintenance of standards globally ensures the following two things:

1) Helps the users as well as developers to find out the best protocol for any application in the field of IoT and
2) It is important so that it can fast-track the outspread of IoT technology in the world.

Detailed summary of IoT standards has been tabulated in Table III.

2) Trends in Internet of Things

The main focus of IoT is to put strain on the interactions among various networked things. The long-term goal of IoT is to make a fusion of Internet and sensing in order to make networked things more smart, flexible, and autonomous so that no human intervention requires. Distinct emerging research technologies in Internet of Things are depicted in Fig. 5.

B. Service-Oriented Architecture

Service-oriented architecture (SoA) should be able to remove the gap between the virtual and physical world. Designing the architecture for IoT involves factors like communication, networking, business models, security, etc. [16]. Few parameters should be taken into

Fig. 5. Emerging research technologies in internet of things.

consideration while designing the IoT architecture, which are scalability and interoperability of heterogeneous devices because they will pass globally and reach out to others in real-time. Hence, their adaptability is a topic of concern.

Thus, SoA takes care of interoperability of these heterogeneous devices in various ways [17-19]. Following are description of the layers:

1) Sensing layer: Its function is to automatically sense the surroundings and exchange data among various hardware devices.

Aspects to be taken care of while determining the sensing layer are shown in Fig. 6.

1) Network layer: It is responsible for providing the connection among devices either through wired or wireless medium.
2) Service layer: It takes care of the services needed by the clients or the applications. It depends on middleware technology. It directly runs on network to find new services for an application.
3) Interface layer: It involves various methods for interaction between the users. This layer is must because heterogeneous devices from multiple vendors face compatibility issues. Thus, to ensure compatibility among them, this layer is implemented, for example, universal plug and play.

A common SoA is shown in Fig. 7 [20].

C. Technologies Enabling Internet of Things

1) **RFID technologies:** The IoT concept was invented on radio frequency-enabled tracking technologies. RFID system usually comprises an RFID tag and an RFID reader. Because of its ability to trace and track, it has been applied in healthcare applications, sales applications, etc. This technology can be used with IoT.

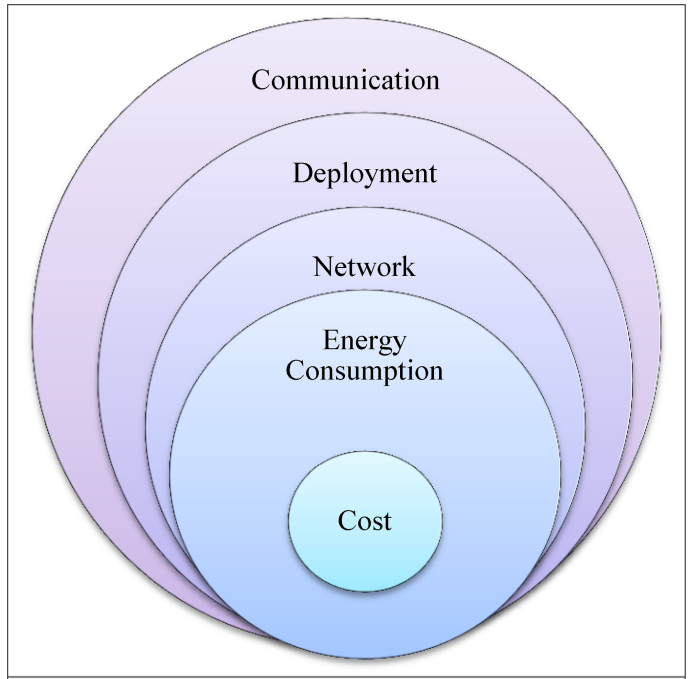

Fig. 6. Factors to be considered for sensing layer.

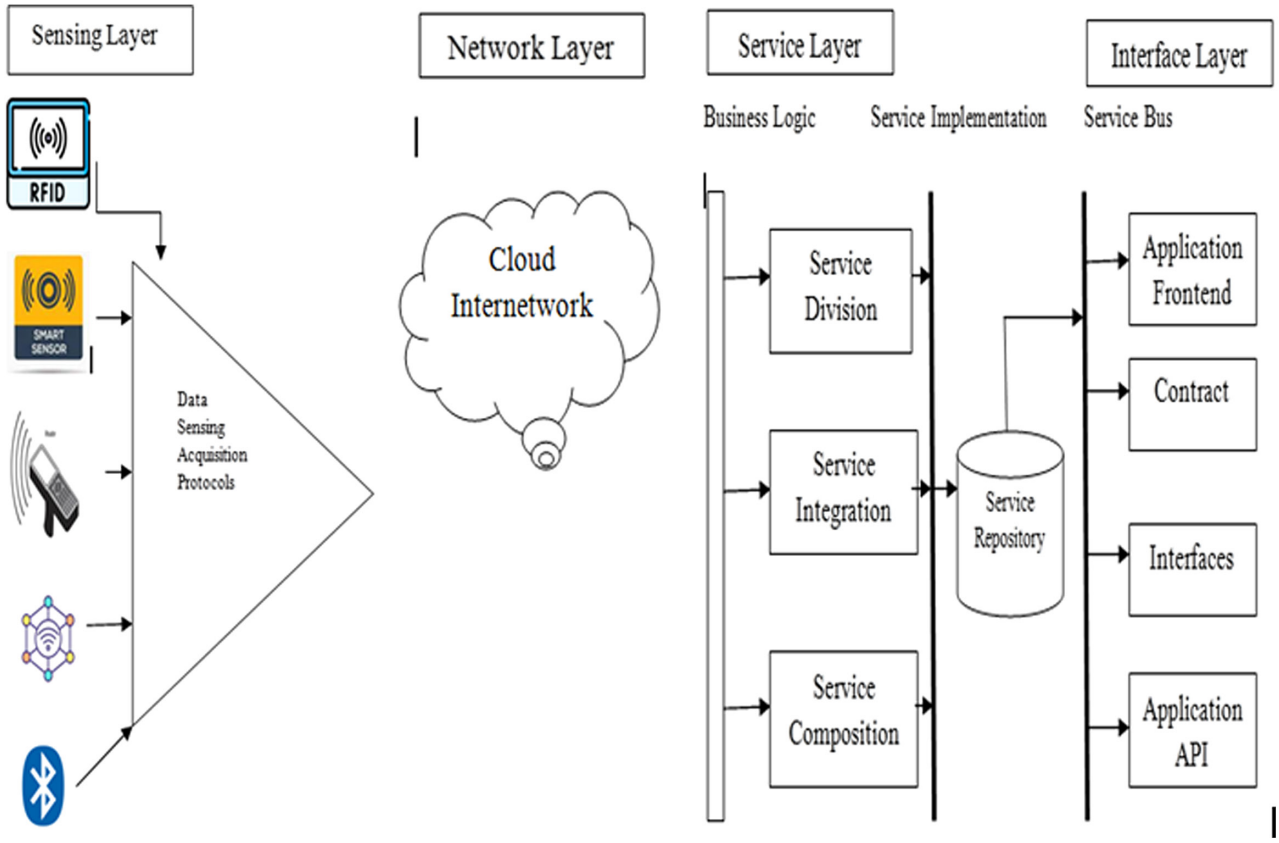

Fig. 7. SoA for internet of things.

2) **Communication:** An IoT consists of many heterogeneous hardware devices and networks like mesh networks, wireless sensor networks, etc. These devices should be well organized and be available through suitable communication mediums. Traditionally, these devices are organized by using gateways over the Internet. In IoT, in order to provide a centralized decision, these gateways must ensure reliable communication [21]. Table IV explains various communication protocols and their standards.
3) **Coalescing of wireless sensor networks and radio frequency identification**
4) **Networks**
5) **Service management:** This term defines how to manage the services that fulfill the needs of the applications and users. SoA promotes the execution of protocols and allows heterogeneous devices to be a part of IoT, thus, benefitting from the failures.

TABLE IV. COMMUNICATION PROTOCOLS WITH THEIR RANGE AND TRANSMISSION RATE

Protocols	Transmission Range	Transmission Rate
Zigbee	10 m	256 kbps/20 kbps
RFID	>50 cm	424 kbps
Bluetooth	10 m	1 Mbps
Wi-Fi	100 m	50–320 Mbps
UMTS/CDMA/EDGE	50 km	2 Mbps

A platform named open service gateway initiative furnishes a dynamic SoA supporting various smart services as described in [22]. Its applications involve areas like plug-ins, mobile apps, etc. A lot of architectures related to service management and IoT have been shown in literature like IBM's architecture using radio frequency identification edge controller. Architecture based on radio frequency identification sensors and readers is explained in [23]. Since IoT is service-oriented, each physical and virtual element can directly interact with other elements providing a transparent service to other elements. SoA provides an easy way for the elements to recommend its functionalities as a service. Organization of these services is done by uniquely identifying them by virtual element. The classification of services is shown in Fig. 8.

6) **Privacy and Security:** Nowadays, two challenges faced by IoT are privacy and security. In order to integrate the output of sensors, efficient security and privacy mechanisms are necessary. In radio frequency identification systems, a large number of authentication protocols have been explained in literature.
A method named "block tag" has been defined for preventing unauthorized access. Also, Tiny Encryption Algorithm (TEA) algorithm and Advanced Encryption Standard (AES) standard have also been proposed to protect the data during exchange. These provocations in privacy and security can be dangerous to user's privacy, access control, authentication of data, etc.

D. Applications

IoT plays an important role in collecting, transmitting, and storing the information that is obtained from sensors. These sensors have

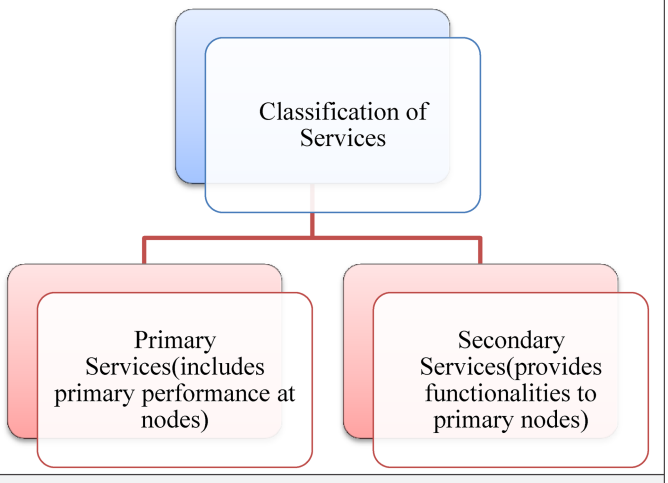

Fig. 8. Classification of services.

major applications in manufacturing, food industry, healthcare monitoring, travel industry, and many more [24].

Its applications are defined in Fig. 9.

E. Challenges in IoT

Since the domain of IoT is vast, it finds applications in various fields like manufacturing, infrastructure, smart agriculture, health care, utility management, etc. Nowadays, the trend is to connect infrastructure of IoT with cloud computing, fog computing, and blockchain in order to complement the capability of IoT. This in turn increases the complexity of IoT networks, thus, demanding security mechanisms to protect the huge amount of data generated by the heterogeneous devices that comprise an IoT network [25].

Security challenges in IoT are classified into five main categories and explained in Fig. 9.

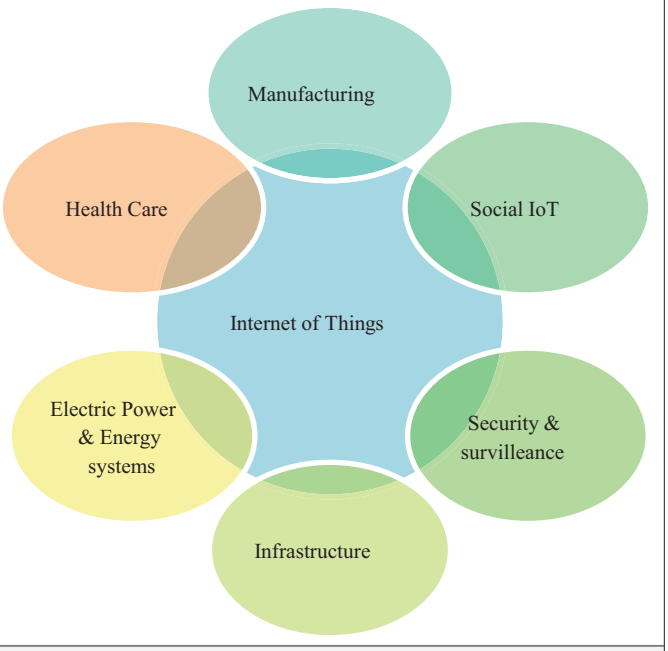

Fig. 9. Application of IoT in current world.

F. Literature Survey on Denial of Service and Insider Attack Detection

The majority of IoT applications are affected by DoS attacks and it will lead to catastrophic effects. Denial of service (DoS) attacks make the services unavailable, thus, changing its normal operation to upside-down. These attacks are done by multiple attackers at the same time, thus making the detection of them before the availability of service become tough.

1) Key Issues in DoS:

1) Detection of insider attack,
2) Efficient denial of service attack detection, and
3) Countermeasures techniques.

Literature survey of the work done in protecting the network from denial of service attack is given in Table V.

2) Future Directions

Most of the frameworks proposed are based on detecting engines and monitoring systems. Implementation of detection engine is mostly on AI-based algorithms over IoT networks. Hence, other efficient lightweight solutions are required for detecting DoS attacks. Another solution can be the use of software-defined networks as they monitor the network at the controller. A hybrid solution can be made by integrating Software Defined Networks (SDN) solutions with the IoT gateways.

G. Literature Survey on Privacy

Privacy is another important security challenge on which more research is required. Since IoT has its applications in numerous fields like traffic control, smart agriculture, smart parking systems, remote patient monitoring, etc., the protection of data in all these fields is a major area of concern.

1) Key Issues in Privacy:

1) Transmission of data securely,
2) Disallowing the identity of an individual while transmitting through the networks as it may lead to threats, and
3) Designing the protocols that do not show the individual's identity, location, time, and space without permission. This is a major concern.

TABLE V. LITERATURE SURVEY FROM DENIAL OF SERVICE ATTACK

[26]	A mechanism has been proposed for monitoring the network consistently with the help of a node. A dynamic threshold is maintained by analyzing the packet loss in real-time, thereby, reducing the loss related to false alarm.
[27]	A detection system known as RADS has been proposed which detects Sybil attacks in 802.15.4 by monitoring.
[28]	Authors formed a framework that spreads in an existing network to prevent fake messages. Adjunct nodes are helpful in monitoring the state of a particular network and implementing the suitable actions that are required at an instant in time.
[29]	TESLA broadcast protocol (DoS tolerant) for the source authentication in IoT has been presented
[30]	An artificial intelligence-based approach with automata-based preventive mechanism is utilized for solving the problem of denial of service attack. But this mechanism is difficult to implement for an IoT network with multiple types of devices.

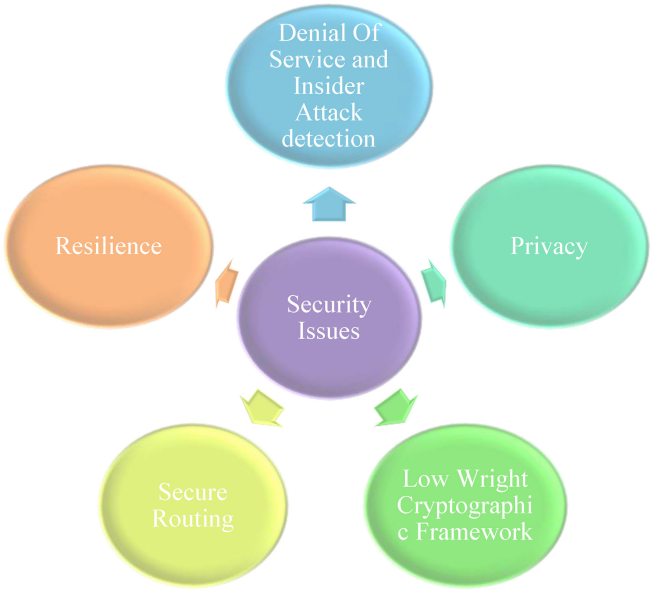

Fig. 10. Security issues in internet of things.

Literature survey of the work done in ensuring privacy is tabulated in Table VI.

2) Future Direction

1) Network virtualization with the help of software-defined networking can be emerged as a solution to privacy by controlling the whole network from a centralized location.
2) A comprehensive framework can be made that can ensure privacy for a large number of applications, and
3) oncept of Game theory can be used for ensuring privacy in data mining and network security. A detailed analysis of game theories has been discussed.

H. Literature Survey on Robustness and Resilience

The network of IoT consists of heterogeneous devices and managing them is not an easy piece of work. Thus, SoA has been developed for its management. But this SoA is prone to almost all the faults in distributed systems like DoS attack, thus disordering the IoT services for the clients.

1) Key Issues in Resilience

1) Network designs inherent to intrusions as well as to other malware attacks are required and
2) Failures occur in each type of network design. Hence, requirement of the architecture is there that can detect and correct the failures at proper time interval. In few applications of IoT, timely management of failures is necessary otherwise, it can lead to life-threatening situations like in disaster management applications.

Literature survey of the work done in ensuring the resilience and robustness of IoT networks is tabulated in Table VII.

2) Future Directions

Making the network to be robust is the major demand of today's network. Various fault-tolerant protocols are there, but the best way to tackle them is by centralizing the network. Thus, better solutions are required to detect the fault at proper time and then choose the best alternative to divert the traffic by the controller.

TABLE VI. LITERATURE SURVEY ON PRIVACY

[31]	A survey related to IoT applications has been done. It has been analyzed that data collected from the sensors record the location and time-related information. Threats to the privacy of user due to authorized access of data have also been discussed.
[33]	The authors explained identity privacy, forward security, backward security, privacy related to location as the privacy and security requirements in cloud-based IoT.
[33]	The authors suggested a security architecture for smart home system. Initially, the gateway architecture is used for smart home purpose. Middleware and cloud architecture has also been surveyed.
[34]	The authors analyzed the security and privacy threats at each hierarchical level of architecture showing the major threat issues such as man-in-the-middle, eavesdropping, etc.
[35]	Security issues like sharing of wireless medium, dynamic network topology, and network architecture (peer to peer) are discussed in Ad hoc networks. A multifence security system has been developed for getting the network performance as desired.
[36]	The paper explains the data tagging method through information flow control in order to manage privacy.
[37]	A key management mechanism using multimedia internet keying protocol and host identity protocol has been provided so that the various IoT devices can be easily distinguished.
[38]	The authors provided a survey on the analysis of the threats by classifying them into seven categories—profiling, localization and tracking, identification, inventory attacks, life cycle transitions, linkage, and privacy violation presentation. The authors concluded the profiling as one of the major threat.
[39]	A path Jumbling method has been explained to preserve the privacy of the users.
[40]	Three sensing applications—personal sensing, community sensing, and designated sensing for wireless community networks (a combination of wireless sensor networks, mobile communication, and wireless mesh networks) have been explained.
[41]	The paper provided the protection of privacy by proposing DTLS-PSK and HIP-PSK for secure communication.
[42]	A survey showing the privacy and trust issues in IoT has been done by the authors. There is a requirement for a dynamic architecture to deal with various hazards that occur due to a large number of interconnected gadgets. The authors also discussed various challenges and convincing solutions too.
[43]	Data manipulation and cryptographic techniques have been used to protect the user in home automation networks.

HIP-PSK, Host Identity Protocol- Pre shared Key; DTLS-PSK, Datagram Transport Layer Security- Pre shared Key

III. CONCLUSION

This survey study initially defined the concept related to resilience differentiation in communication services. The basic terminologies, attributes, and recovery mechanisms of resilience differentiation

TABLE VII. LITERATURE SURVEY ON ROBUSTNESS AND RESILIENCE

[44]	The authors presented a protocol called efficient coopertive security which controls the entry and calling off of the nodes by using two procedures. Security has been provided to IoT devices to ensure resilience.
[45]	The authors implemented an approach based on artificial intelligence to tolerate the faults by presenting a fault-tolerant protocol based on learning automata.
[46]	A self-optimizing and fault-tolerant network management framework has been shown by authors for wireless sensor networks.
[47]	The authors have shown a fault detection system for monitoring the industrial IoT based on self-learning.

have been introduced in order to implement the same in terms of IoT. IoT plays a major role in today's life. Due to the utilization of heterogeneous devices, IoT suffers from various threats, reliability issues, fault-tolerant issues, resilience issues, privacy issues, secure routing and forwarding issues, etc.

The work in this study has been intended to provide awareness about various emerging trends and challenges in IoT so that a more creative and advanced solution can be made for the advancements in IoT. Fault tolerance management by using novel techniques of active and passive replication for quality of service (performance and availability) can be a challenging topic. Apart from that, SoA and microservice architecture can be further investigated for these parameters.

Peer-review: Externally peer-reviewed.

Author Contributions: Concept – S.S.; Supervision – B.K.P., R.K.; Data Collection and/or Processing – S.S.; Analysis and/or Interpretation – S.S., B.K.P., R.K.; Literature Review – S.S., B.K.P., R.K.; Writing – S.S.; Critical Review – B.K.P., R.K.

Declaration of Interests: The authors have no conflicts of interest to declare.

Funding: The authors declared that this study has received no financial support.

REFERENCES

1. V. S. Pana, O. P. Babalola, V. Balyan, "5G radio access networks: a survey", *Array Elsevier*, vol.14, pp. 1–10, 2022.
2. O. P. Babalola, and V. Balyan, "Vertical handover prediction based on hidden markov model in heterogeneous VLC-wiFi system", *Sensors-MDPI*, Vol. 22, no. 7, 2022.
3. P. Cholda, A. Mykkeltveit, B Helvik, O Wittner, and A Jajszczyk, "A survey of resilience differentiation frameworks in communication networks," *IEEE Commun. Surv. Tutor.*, vol. 9, no. 4, pp. 32–55, 2007. [CrossRef]
4. P. Demeester et al.,"Resilience in multilayer networks," *IEEE Commun. Mag.*, vol. 37, no. 8, pp. 70–76, 1999. [CrossRef]
5. D. Papadimitriou, and E. Mannie, Eds., "Analysis of generalized multi-protocol label switching (GMPLS)-based recovery mechanism (including protection and restoration)," *IETF RFC*, vol. 4428, pp. 1–47, 2006.
6. S. Orlowski, and R. Wessäly, "Comparing restoration concepts using optimal network configurations with integrated hardware and routing decisions," *J. Netw. Syst. Manag.*, vol. 13, no. 1, pp. 99–118, 2005. [CrossRef]
7. P-H Ho, J. Tapolcai, and T Cinkler, "Segment shared protection in mesh communications networks with bandwidth guaranteed tunnels," *IEEE ACM Trans. Netw.*, vol. 12, no. 6, pp. 1105–1118, 2004. [CrossRef]
8. T. Van Landegem, P. Vankwikelberge et al., "A self- healing ATM network based on multilink principles," *IEEE J. Sel. Areas Commun.*, vol. 12, no. 1, pp. 149–158, 1994.
9. H. Fujii, and N. Yoshikai, "Restoration message transfer mechanism and restoration characteristics of double-search self-healing ATM network, " *IEEE J. Sel. Areas Commun.*, vol. 12, no. 1, pp. 149–158, 1994. [CrossRef]
10. S A El Shazely, O A M Abdel Mohsen, and K Shehatta, "Enhancing MPLS network fault recovery using P-Cycle with QoS protection," ITI 5th International Conference on Information and Communications Technology, 2007, pp. 197–202. [CrossRef]
11. D. Colle *et al.*, "Data-centric optical networks and their survivability," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 1, pp. 6–20, 2002. [CrossRef]
12. W. D. Grover, *Mesh-Based Survivable Networks- Options and Strategies for Optical, MPLS, SONET, and ATM Networks*. Prentice Hall PTR, 2004.
13. "Internet protocol data communication service — IP packet transfer and availability performance parameters," *ITU-T Rec. Y.1540*, 2002.
14. "Terms and definitions related to quality of service and network performance including dependability," *ITU-T Rec. E.800*, 1994.
15. B. Jaeger, and D. Tipper, "Prioritized traffic restoration in connection oriented QoS based networks," *Comput. Commun.*, vol. 26, no. 18, pp. 2025–2036, 2003. [CrossRef]
16. J. Ulmer, J. Belaud, and J Le Lann, "A pivotal-based approach for enterprise business process and IS integration," *Enterpr. Inf. Syst.*, vol. 7, no. 1, pp. 61–78, 2013. [CrossRef]
17. H. Panetto, and J. Cecil, " Information systems for enterprise integration, interoperability and networking: Theory and applications, " *Enterpr. Inf. Syst.*, vol. 7, no. 1, pp. 1–6, 2013. [CrossRef]
18. X V Wang, and X W Xu, "DIMP: An interoperable solution for software integration and product data exchange, "*Enterpr. Inf. Syst.*, vol. 6, no. 3, pp. 291–314, 2012. [CrossRef]
19. R. Jardim-Goncalve, A. Grilo, C Agostinho, F Lampathaki, and Y Charalabidis, "Systematisation of interoperability body of knowledge: The foundation for enterprise interoperability as a science," *Enterpr. Inf. Syst.*, vol. 7, no. 1, pp. 7–32, 2013. [CrossRef]
20. J. H. Krapelse, "RFID application in healthcare – scoping and identifying areas for RFID deployment in healthcare delivery," *Rand Europe*, 2009.
21. D. Miorandi, S. Sicari, F De Pellegrini, and I Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1497–1516, 2012. [CrossRef]
22. K. Gama, L.Touseau, and D Donsez, "Combining heterogeneous service technologies for building an Internet of things middleware," *Comput. Commun.*, vol. 35, no. 4, pp. 405–417, 2012. [CrossRef]
23. W. Tan, W. Xu, F Yang, L Xu, and C Jiang, "A framework for service enterprise workflow simulation with multi-agents cooperation, " *Enterpr. Inf. Syst.*, vol. 7, no. 4, pp. 523–542, 2013. [CrossRef]
24. B. Xu, and L. Xu et al., "Ubiquitous data accessing method in IoT-based information system for emergency medical services," *IEEE Trans. Ind. Inform.*, pp. 1578–1586, 2014.
25. A. Kanuparthi, R Karri, and S Addepalli, "Hardware and embedded security in the context of internet of things," in Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles, 2013, pp. 61–64. [CrossRef]
26. Y. Hu, Y. Wu, and H Wang, "Detection of insider selective forwarding attack based on monitor node and trust mechanism in WSN," *Wirel. Sens. Netw.*, vol. 06, no. 11, pp. 237–248, 2014. [CrossRef]
27. P. Sarigiannidis, E. Karapistoli, and A A Economides, "Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information," *Expert Syst. Appl.*, vol. 42, no. 21, 7560–7572, 2015. [CrossRef]
28. D. Juneja, and N. Arora, "An ant based framework for preventing DDoS Attack in wireless sensor networks," *Int. J. Adv. Technol.*, vol. 1, no. 1, pp. 34-44, 2010.
29. N. Ruan, and Y. Hori, "DoS attack-tolerant TESLA-based broadcast authentication protocol in Internet of things," in Proceedings of International Conference on Selected Topics in Mobile and Wireless Networking, 2012, pp. 60–65. [CrossRef]
30. S. Misra, P. V. Krishna, H Agarwal, A Saxena, and M S Obaidat, "A learning automata based solution for preventing distributed denial of service in internet of things," in Proceedings of International Conference on Internet of 5ings and 4th International Conference on Cyber, Physical and Social Computing, 2011, pp. 114–122. [CrossRef]
31. J. Zhou, Z. Cao, X Dong, and A V Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, 2017. [CrossRef]

32. D. Christin, A. Reinhardt, S S Kanhere, and M Hollick, "A survey on privacy in mobile participatory sensing applications," *J. Syst. Softw.*, vol. 84, no. 11, 1928–1946, 2011. [CrossRef]
33. H. Lin, and N. Bergmann, "IoT privacy and security challenges for smart home environments," *Information*, vol. 7, no. 3, pp. 2016. [CrossRef]
34. J. Veijalainen, D. Kozlov, and Y Ali, "Security and privacy threats in IoT architectures," in *Proceedings of 7th International Conference on Body Area Networks*, 2012. [CrossRef]
35. H. Yang, H. Luo et al., "Security in mobile ad hoc networks: Challenges and solutions," *IEEE Wirel. Commun.*, vol. 11, no. 1, pp. 38-47, 2004.
36. D. Evans, and D. M. Eyers, "Efficient data tagging for managing privacy in the internet of things," in Proceedings of 2012 IEEE International Conference on Green Computing and Communications, 2012, pp. 244–248. [CrossRef]
37. F. V. Meca, J. H. Ziegeldorf et al., "HIP security architecture for the IP-based internet of things," in Proceedings of IEEE Advanced Information Networking and Applications Workshops (WAINA), pp. 1331–1336, 2013.
38. J. H. Ziegeldorf, O. G. Morchon, and K Wehrle, "Privacy in the internet of things: Threats and challenges," *Sec. Commun. Netw.*, vol. 7, no. 12, pp. 2728–2742, 2014. [CrossRef]
39. D. Christin, A. Reinhardt et al., "On the efficiency of privacy-preserving path hiding for mobile sensing applications," in Proceedings of IEEE LCN, 2013.
40. D. Christin, M. Hollick, and M Manulis, "Security and privacy objectives for sensing applications in wireless community networks," in Proceedings of ICCCN, 2010, pp. 1–6. [CrossRef]
41. O. Garcia-Morchon, S. L. Keoh, S Kumar, P Moreno-Sanchez, F Vidal-Meca, and J H Ziegeldorf, "Securing the IP based internet of things with HIP and DTLS," in Proceedings of Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2013. [CrossRef]
42. S. Sicari, A. Rizzardi, L A Grieco, and A Coen-Porisini, "Security, privacy and trust in Internet of things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, 2015. [CrossRef]
43. M. R. Schurgot, D. A. Shinberg, and L G Greenwald, "Experiments with security and privacy in IoT networks," in Proceedings of IEEE World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015, pp. 1–6. [CrossRef]
44. D. Kuptsov, A. Gurtov, O Garcia-Morchon, and K Wehrle, "Brief announcement: Distributed trust management and revocation," in Proceedings of 29th ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing, 2010. [CrossRef]
45. S. Misra, A. Gupta, P V Krishna, H Agarwal, and M S Obaidat, "An adaptive learning approach for fault tolerant routing in internet of things," in Proceedings of 2012 IEEE Wireless Communications and Networking Conference (WCNC), 2012, pp. 815–819. [CrossRef]
46. M A Rajan, P. Balamuralidhar, K P Chethan, and M Swarnahpriyaah, "A self-reconfigurable sensor network management system for internet of things paradigm," in Proceedings of 2011 International Conference on Devices and Communications (ICDeCom), 2011, pp. 1–5. [CrossRef]
47. Y. Liu, Y. Yang, X Lv, and L Wang, "A self-learning sensor fault detection framework for industry monitoring IoT," *J. Comput. Netw. Commun.*, vol. 2013, 712028, 2013. [CrossRef]

Shalini Sharma – She received Bachelor of Technology degree from Baddi University of Emerging Sciences and Technology, India, in 2016. She received M.Tech from Shoolini University of Biotechnology and Management Sciences, India, in 2019. Her areas of interest in research are Optical Fibers and IoT Networks.

Bhupendra Kumar Pathak – Dr. Bhupendra Kumar Pathak has completed his doctorate degree in the area of operation research from the department of Mathematics, Dayalbagh Educational Institute (Deemed University), Dayalbagh, Agra, India, in 2007 under the supervision of Prof. Sanjay Srivastava. His present research interests include soft computing techniques such as neural network, fuzzy logic, and evolutionary computation methods. He has published several research papers in national and international peer-reviewed journals. He is associated with Jaypee education system since June 2011. Before joining the Jaypee Education System, he was associated with ITM University, Gurgaon, from August 2009 to June 2011, AMITY University, Noida, from January 2008 to July 2009 and R.B.S. Degree College, Agra, from 2003 to December 2007.

Dr. Rajiv Kumar – He received Bachelor of Technology from College of Technology, G.B. Pant University of Agriculture and Technology, Pant Nagar, India, in 1994. He received M.Tech. from NIT Kurukshetra (formerly REC, Kurukshetra), India, in 2001. He received his Ph.D. degree from NIT Kurukshetra in the year 2010. His areas of interest in research are networks and systems.