IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.6, Issue.10, Oct. 2018 E-ISSN: 2347-2693

A Survey on Trust-based Intrusion Detection for Version Number Attack on RPL

Hiral Patel[1*], Hiren Patel[2], Bela Shrimali [3]

[1,2,3]Dept. of Computer Engineering, LDRP Institute of Technology & Research, Gandhinagar, India

[*]*Corresponding Author: hirallakani@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 17/Oct/2018, Published: 31/Oct/2018

***Abstract*—** The IoT incorporates the network of physical devices (things) that are connected to the global Internet for transferring and performing computation in lager application area. Routing protocols are designed for Low Power and Lossy network (RPL) to support communication in the constrained network with thousands of such power-scarce nodes in IoT. Consequently, due to the increases in millions and billions of connected devices in the constraint network(s) all over the world, security has become the aspect of most significance. Lightweight Intrusion Detection System (IDS) is required to examine the malicious activity and malicious node in the network of IoT, to filter out different attacks in a resource-constrained environment. In this paper, the lightweight trust based intrusion detection methods covering the different attacks of the wireless sensor network and IoT are reviewed and discussed. This article may give the direction to the beginners to identify appropriate methods and observations for their future research in the application domain of IoT.

***Keywords*—** IoT, RPL, security, attacks, Trust-based, intrusion detation

I. INTRODUCTION

Internet of Things (IoT) enables the devices to be smart and creates the network where these devices may uniquely identify and communicate with each other without human interference [1]. These smart devices are used in an enormous number of IoT applications like home automation, healthcare, agriculture, transportation, retail and logistics, industrial and environment etc [2]. Thus, IoT will bring inconceivable benefits and make human life smarter and luxurious. But, these benefits come with new security threats or attacks on IoT that need to be addressed.

The IoT devices are interconnected for exchanging the information through Internet. They are identified and share the information using routing protocol. The route between smart devices to transfer the data is identifying by the routing protocols. There are many scenario where the IoT nodes are having limited power and are operated in a network with high data loss, such network is called Low power and Lossy Network (LLN). A well-known standardized routing protocol in the Wireless Sensor Network (WSN) and IoT is IPv6 Routing protocol for such network known as Routing protocol for Low Power and Lossy Networks (RPL) proposed as the network layer standard by Internet Engineering Task Force (IETF) [3]. RPL is a distance vectored and source routing protocol that constructs Destination-Oriented Directed Acyclic Graph (DODAG) in LLNs. This DODAG is formed via connection of IoT devices, which are interconnected with each other and connecting to the Internet through border router.

Privacy and security are two major concerns in IoT. The data exchanged between IoT devices should temper proof. To ensure privacy and security, different security protocols are required at various layers of IoT. The devices used in IoT are generally power-scare. Hence, the protocol needs to be lightweight in terms of computation and communication cost. Due to the dynamic nature and different types of smart devices, it is difficult to detect and prevent attacks as compared to static network [4]. Under such a scenario, RPL is considered to be an adequate option as far as routing protocols are concerned. RPL includes inbuilt/optional security and fault tolerance mechanisms, such as encryption of control messages, global and local repairs [3]. Broadly, the attacks are classified under two categories viz. internal and external attacks. Intrusion Detection System (IDS) is commonly used to detect and filter such attacks [4]. Usage of IDS in IoT environment requires changes in the IDS architecture due to resource-constrained nature of the devices used in IoT.

Various attacks such as selective forwarding, rank, version, sinkhole, black hole, local repair, wormhole, identity, sniffing, sybil and Denial of Service (DoS) attack etc. can largely be divided into three classifications viz. resource-

based attacks, traffic-based attacks, and network-topology-based attacks in view of RPL protocol [5]. As RPL is normally used with sensor nodes, WSN is the most common sufferer of the attacks mentioned above. To counter different RPL attacks in WSN and IoT, many algorithms and methods have been proposed which use Expected Transmission (ETX) matric link to reliability metric and rank for detection of malicious network nodes and network activities [6]. In one of the types of IDS, Trust-based Intrusion Detection System (TIDS), where nodes of network observe adjacent nodes, build up a measurement about the trustworthiness and try to detect whether or not the neighbour is acting according to the trust policies [7]. In this research, we aim to explore the trust based intrusion detection systems.

This paper is regularized as follows. Section II presents an overview of RPL in IoT and WSN followed by Section III covering related works on RPL attacks with more detailing on version number attack. Section IV present Trust based IDS (TIDS) strategies in WSN and IoT. Section V presents version number attacks and its effect on the network. Section VI presents conclusion and future work.

II. AN OVERVIEW OF RPL

RPL [3] is a proactive routing protocol designed for IoT sensor nodes in low power and lossy networks. It traditionally organizes a logical representation of the network topology as a one or more DODAGs through which data packets are routed. Every node in the RPL network bond to tree like DODAG, which connect with IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) DODAG root known as 6LoWPAN Border Router (6BR). The 6BR is coupled to the Internet, backbone router (BR), other 6BRs or repository. RPL significantly introduce Internet Control Message Protocol for IPv6 (ICMPv6) type 155 control messages viz. DODAG Information Object (DIO), DODAG Information Solicitation (DIS), Destination Advertisement Object (DAO) and Destination Advertisement Object Acknowledgment (DAO-ACK) and trickle mechanism for build and maintaining DODAG network topology. These messages are helpful in the following way:

- DIO control message is initiated by sink node (root) and broadcast to all nodes in the coverage range of the root node for a discovery of the DODAG topology. When RPL network is constructed due to missing of many links in network or time expired, nodes exchange DODAG information via DIO message which helps nodes to select their preferred parent based on different metrics like hop-count, expected transmission count, link reliability and link colour object. The identified parent acts like a gateway for that node.

- DIS is a multicast message towards the neighbouring nodes, when a new node wishes to join the DODAG, and it requires the DIO message from a neighbour within range.

- DAO unicast message is used to propagate information in the upward direction to maintain downward routes in DODAG network. Newly joins node advertises a DAO message for update routing table of their neighbour.

- DAO-ACK is used by the node to propagate information who received DAO message.

RPL [3] has facilitate a rebuild of DODAG topology and during such rebuilds, the parent of some nodes might change in the DODAG tree topology. The movement of the node might be breaking the link of network topology also cause a change in the RPL tree. RPL has two mechanisms to repair the DODAG tree, one is to avoid the loops known as local repair mechanism and another is allowed nodes to join, disjoin or re-join a new position in a network known as a global repair mechanism.

Global repair is an operation mode in which the DODAG root increments the DODAGVersionNumber field in control package. Nodes in the new DODAG version can choose a new position whose rank is constrained by their rank within the old version of DODAG. Whereas, local repair-used to detect loop within the network of DODAG version. For example, the node can isolate from the DODAG, advertise a rank of INFINITE RANK to inform its sub DODAG, and finally re-attach to the original or a brand-new DODAG [3].

RPL [3] identify the selection of better packet route based on the objectives defined by the Objective Function (OF) like hop count, ETX, energy, signal to noise ratio, stability, distance, connectivity etc. for selection of better packet route between nodes of a network. The better result of RPL routing depends on selected OF, which may identified as challenge in RPL routing.

Other identified challenges in RPL are multicasting, load balancing, mobility, security [8] [9]. Among all, security is a major concern, even though it is optional. The major security issues are trust management, bootstrapping, interoperability, scalability, time maintenance, resource provisioning, legacy system, scalability, computation complexity [10]. P. Manickam et al. [11] adders the behavior of the RPL protocol in cooja simulator and its working mechanisms with different data transmission ranges.

III. RELATED WORKS

Intrusion detection is probably the challenging issue in the IoT, and that has been significantly discussed in numerous research works with different simulator and scenario. In this section, we have analysed different attacks on RPL with

different monitoring mechanism. Among all we have more focused on version number attack audits currently available mechanisms for prevention and detection.

A. Mayzaud [12] and R. Mehta et al. [13] surveyed and addressed security attacks, impacts of attacks on network parameters and count measurement to mitigate them on RPL protocol in IoT and WSN associated with different applications.

A. Mayzaud et al. [14] classified existing monitoring architectures in two main categories for detecting malicious activity viz: active and passive monitoring, based on the participation of target nodes in the monitoring task. Based on the decision-making process they have further classified monitoring architectures in centralized, decentralized and hybrid.

A Dvir et al. [15] addressed the security issue of traditional RPL protocol which compromised the security of internal network nodes. For the same, they proposed an algorithm VeRA (Version Number and Rank Authentication in RPL) which aims to mitigate version number and rank spoofing attack by using one-way hash chain and message authentication codes. Due to the dependency of hash chain elements to the pre-image of chain element attacker need to compute the pre-image for increasing the version number or decreasing the rank value of nodes. However, they have not provided sufficient protection to the pre-image of the hash chain element and performance analysis. Overhead generate in the network due to the traditional cryptography algorithms in IoT environment. So, that authors established new security scheme to mitigate attacks.

A. Mayzaud et al. [14] proposed a detection strategy based on distributed monitoring nodes, to mitigate the malicious node activity that increase the version number and propagate alter version number. However, algorithm supports presences of only one malicious node in the constraint network. Proposed algorithm place the multiple monitoring nodes in a network, which periodically share monitoring data to the (root) border node and also report to the root node when increasing of the version number in the neighbourhood is detected. Based on same, the root node collects all node monitoring information and analyzes overall information to identify the attackers. For evaluating the performance of network they implemented the algorithm in a grid and cluster-based topology and simulated in cooja simulator. The author claimed that the proposed algorithm gives better performance in cluster-based topology.
F. Ahmed et al. [16] proposed an algorithm for detection of version number attack based on a distributed and cooperative verification mechanism in IoT environment where less number of malicious node in a network scenario. In this mechanism, when a node receives a DIO message with increased DODAG version number from the neighbour or parent, cooperative verification mechanism at receiving node route message to the maximum two hope limit to verifying the identity of neighbour's and parent. The author claimed that their proposed approach commute network parameter like control packet overhead.

M. Nikravan et al. [17] proposed IBOOS, identity-based cryptosystem to mitigate version number and rank spoofing attacks in IoT and WSN. To mitigate the version number attack they initially allow sink node to acquire only one time own private key, offline sign and some another parameter to secure network. The sink node increases the version number, it signed version number and broadcast it. Node which reserves DIO message verify that signature. If verification is done successfully than it updated its own version number and propagate without changing signature version number otherwise discard it. They claimed that IBOOS schema is more secure and it is an efficacy filter malicious node from the large network with minimum used of a network resource. Where values of rank and the version number is signed independently and to get the private key of nodes is difficult.

IV. TRUST BASED IDS

A reputation system is used mostly now a days due to building a trust among users. For example eBay, Amazon.com, It defined that users to rate the system in order to build trust through reputation. Similarly, in a network of sensor and IoT, it is possible through observation and evaluation of neighbour nodes which are close enough to receive its signal [18]. The nodes assess the neighbour node and try to adjudge if the node is acting according to the trust metric. TIDS is system, where Trusted Platform Module (TPM) is integrated into each network node and nodes rely on a new collaborative trust metric evaluation for routing [19] [20].

Trust estimation and evaluation are an important part of the trust-based schema. There are many different methods to figure out trust degree in IoT, WSN, cloud, cluster and distributed computing. D. Airehrour [7] summarized all possible trust model used in various network.

To improve the security and privacy based on a trustworthiness on RPL, there are two possible way. First, a change in RPL protocol by altering RPL control message or altering selection technique of objective function and second is to embed new mechanism to compute trust with a routing protocol.

To mitigate different types of routing attack on RPL existing monitoring architecture may be classified into three categories based on trust propagation which is used to lead trust opinion to peers. First one is centralized trust [21] [22] propagation, the trust observation is distributed to a centralized entry, a

border router of the network. The second one is distributed trust [21] [22] propagation when IoT devices distribute trust observation autonomously to its neighbours without any central entry. And finally hybrid trust propagation, when distributed and cooperative trust observation combines autonomously with central entry.

ZA Khan et al. [21] proposed a trust-based mechanism to mitigate the selective forward attack, sinkhole attack and version number attack based on centralized trust propagation. And used fuzzy logic to combine trust at the border router. Rank, version number and timer are used as trust matrices to detect attacks. Each node observed trust matrices of the neighbour node to create opinion tringle for trust evaluation and send it to the border router for trust update. Border router aggregate trust to filter out attacker node from the district node using josang subjective logic and check whether or not it goes below a threshold. To propagate trust from nodes to the border router they introduced new RPL control message called Trust Information (TRU) message which hold trust variable and the IP-address of the observed node. However, they did not provide sufficient security of TRU-message. Further, they evaluated their work in MATLAB and Contiki OS [22] and claimed that their mechanism efficiently detects a large number of the attackers with less false negative and false positive judgment.

D. Airehrour et al. [23] addressed the issues of computation resource in cryptography and authentication based intrusion detraction mechanism in IoT. For the same, they integrated trust-aware mechanism with RPL protocol and detected blackhole and selective forwarding attacks. That further used for routing decision. They discussed distributed propagation mechanism, where the new DODAG is created based on the node parameters and trust value. They calculate trust value based on feedback based observation of trust parameters and stored in descending order for selecting preferable routing decision. They implemented proposed mechanism in cooja simulator and measures different network parameter.

F. Medjek et al. [24] proposed a hybrid trust-based propagation system on RPL to detect intrusion node in the network of DODAG which creates sybil attack. The authors combined three modules: identity, mobility and IDS module with modifying DIO message format. Identity module provided a unique identity to every node in the DODAG tree, handles the identity issue and off-lode security feature by RSA based trusted platform module (TPM). Mobility module handled the mobility of a node within a network and obtains the localization of the mobile malicious node in the network. After verifying above two module, IDS module at network node allowed to calculate the trust values up to one-hop neighbors for filter out and discard the malicious nodes. Node informs to another node about malicious node by propagating multicast message. Authors ensure proposed system efficiently handle the static as well as a mobile attacker in RPL.

J. Caminha et al. [25] proposed a system based on machine learning and elastic slide window technique to determine the trust from IoT object and filter the malicious nodes. They claimed that proposed system is able to detect an on-off attack in real-world IoT environment and cooja simulator.

V. VERSION NUMBER ATTACK AND IT'S EFFECT

Version number and rank are two main terminologies in RPL package to maintain network topology. A version of DODAG is a definite iteration (version) of a DODAG with corresponding DODAGID and it is part of DIO control message. Rank of node defines individual node positions with respect to the DODAG root. In the global repair process of RPL, the sink node of the network used version number to determine that all nodes in the DODAG are up-to-date with the routing state. So, when the sink node propagates a new version number, the nodes which contain older DODAG version need to join the new DODAG by stored new version number and rank [26].

Figure 1 illustrate a rebuilding of DODAG under scenario of global repair process accurses in a network. The new DODAG topology is being built represented by red solid arrows, old DODAG topology is represented by blue solid arrows, DOI message propagation is represented by green dashed arrows and an available link between nodes of DODAG are represented by a black dashed line.

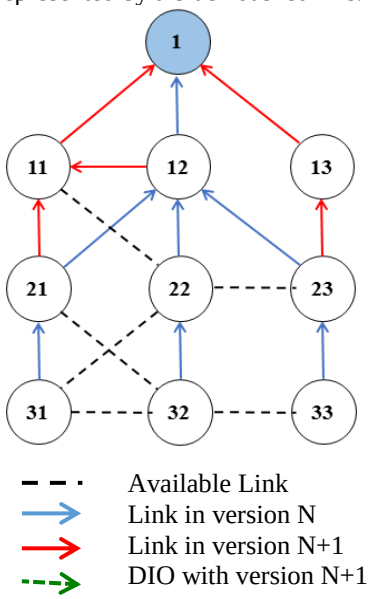

Figure 1. Example of New DODAG iteration

During the global repair process, it is a possible to have two version of DODAG coexists in the network responds to create loops. So, the version number should be unchanged during

propagation of DIO message through the DODAG. However, there is no mechanism in RPL to check the version number integrity in DIO messages [26].

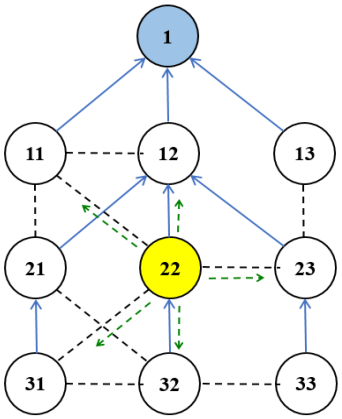

Figure 2. Malicious node DIO message propagation

To harm the DODAG network, malicious node alter a version number field in its own DIO message and propagate DIO control message to the neighbour as represented in Figure 2. Nodes receiving DIO message with a new version number, will reset version number and rank in their own records and advertise malicious DIO message to their neighbourhoods. So, a malicious DIO message generates an unnecessary rebuild of DODAG and generates loops in the network topology [26].

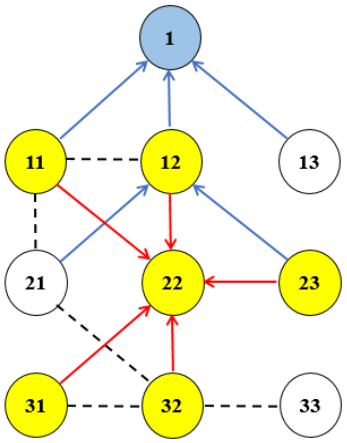

Figure 3. Example of propagation of alter version number

A. Aris [27] claimed that due to the version number attack packet delivery ration, control packet overhead and end-to-end delay of a network are increased and their rate of change directly proposed to the location of the attacker.

VI. CONCLUSION

Due to the wide use of IoT and WSN worldwide, the security is come up as major concern factor. In this paper, we have discussed the concept of RPL and version number attack and discussed the effect of version number attack in the RPL network. Further, we have discussed the different mechanisms of version number attacks available in current state-of-an-art. Moreover, we have also analysed varies technique of TIDS applicable to different attacks. It has been analysed that trust-based system is more efficient in terms of computation and security compared to the without-trust-based system. As, verification and encryption - deception process is executed in without trust for each communication. Future work may involve an alternative smart trust based technique that can detect version number attacks with preservation of speed of RPL routing protocol and system resources.

REFERENCES

[1] H.D. Ma., "Internet of things: Objectives and scientific challenges", Journal of Computer science and Technology, Vol. 26(6), pp.919–924, 2011.
[2] L. Patra, U.P. Rao, "Internet of Things - Architecture, applications, security and other major challenges", 2016 3rd International Conference on Computing for Sustainable Global Development, New Delhi, pp. 1201-1206, 2016.
[3] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, Internet Engineering Task Force, 2012.
[4] L. Wallgren, S. Raza, T. Voigt, "Routing Attacks and Countermeasures in the RPL-based Internet of Things" International Journal of Distributed Sensor Networks, Vol. 9(8), p. 794326, 2013.
[5] B.A. Alabsi, M. Anbar, S. anickam, "A Comprehensive Review on Security Attacks in Dynamic Wireless Sensor Networks based on RPL protocol", International Journal of Pure and Applied Mathematics, Vol.118, pp. 653-667, 2018.
[6] D. Shreenivas, S. Raza, T. Voigt, "Intrusion Detection in the RPL-connected 6LoWPAN Networks", ACM International Workshop on IoT Privacy, Trust and Security, pp. 31 – 38, 2017.
[7] D. Airehrour, "A Trust-based Routing Framework for the Internet of Things", PhD Diss, Auckland University of Technology, 2017.
[8] H.S. Kim, J. Ko, D.E. Culler, J. Paek, "Challenging the IPv6 Routing Protocol for Low Power and Lossy Networks (RPL): A Survey", IEEE Communications Suveys and Tutorials, Vol. 19, No. 4, pp. 2502 –2525, 2017.
[9] M. Kaur, A. Mohd Aslam, "Big Data Analytics on IOT: Challenges, Open Research Issues and Tools", International Journal of Scientific Research in Computer Science and Engineering, Vol.6, Issue.3, pp.81-85, 2018.
[10] C. Bekara, "Security Issues and Challenges for the IoT-based Smart Grid", International Workshop on Communicating Objects and Machine to Machine for Mission Critical Application, Elsevier, pp. 532 – 537, 2014.
[11] P. Manickam, V. Muthu Ganeshan, M. Girija, "Comprehensive Approach in Studying the Behaviour of Contiki RPL Protocol in Diverse Data Transmission Ranges", International Journal of Scientific Research in Network Security and Communication, Vol. 6, Issue. 3, pp. 37-42, 2018.
[12] A. Mayzaud , R. Badonnel, I. Chrismen, "A Taxonomy of Attacks in RPL-based Internet of Things", International Journal of Network Security, Vol.18, No. 3, pp. 459 – 473, 2016.
[13] R. Mehta, M.M. Parmar, "A Survey on Security Attacks and Countermeasures in RPL for Internet of Things", International

Journal of Advance Research in Science and Engineering, Vol. 7, No. 3, 2018.
[14] A. Mayzaud, R. Badonnel, I. Chrisment, "A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-Based Networks", IEEE Transactions on Network and Service Management, Vol. 14, No. 2, pp. 472-486, 2017.
[15] A. Dvir, T. Holczer, L. Buttyan, "VeRA - Version Number and Rank Authentication in RPL", 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, Valencia, pp. 709-714, 2011.
[16] F. Ahmed, Y.B. Ko, "A Distributed and Cooperative Verification Mechanism to Defend against DODAGVersion Number Attack in RPL", International joint conference on Pervasive and Embedded Computing and Communication systems, Vol. 1, pp. 55–62, 2016.
[17] M. Nikravan, A. Moaghar, M. Hosseinzadeh, "A Lightweight Defense Approach to Mitigate Version Number and Rank Attacks in Low-Power and Lossy Networks", Wireless Personal Communications, Springer, pp. 1 –25, 2018.
[18] C.R. Perez-Toro, R.K. Panta, S. Bagchi, "RDAS: Reputation-Based Resilient Data Aggregation in Sensor Network", 2010 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), Boston, MA, pp. 1-9, 2010.
[19] N. Djedjig, D. Tandjaoui, F. Medjek, "Trust-based rpl for the Internet of things", in 2015 IEEE Symposium on Computers and Communication (ISCC). IEEE, pp. 962–967, 2015.
[20] N. Djedjig, D. Tandjaoui, F. Medjek, I. Romdhani, "New trust metric for the rpl routing protocol", in 2017 IEEE The 8th International Conference on Information and Communication Systems (ICICS). IEEE, 2017.
[21] Z.A. Khan, P. Herrmann, "A Trust Based Distributed Intrusion Detection Mechanism for Internet of Things", 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), Taipei, pp. 1169-1176, 2017.
[22] F. Nygaard , "Intrusion Detection System In IoT", Master's thesis, NTNU, 2017.
[23] D. Airehrour, J. Gutierrez, S.K. Ray, "A Trust-Aware RPL Routing Protocol to Detect Blackhole and Selective Forwarding Attacks", Australian Journal of Telecommunications and the Digital Economy, vol. 5, April 2017.
[24] F. Medjek, D. Tandjaoui, I. Romdhani, N. Djedjig, "A Trust-Based Intrusion Detection System for Mobile RPL Based Networks", 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, pp. 735-742, 2017.
[25] J. Caminha, A. Perkusich, M. Perkusich, "A Smart Trust Management Method to Detect On-Off Attacks in the Internet of Things", Security and Communication Networks, pp.10, 2018.
[26] A. Mayzaud, R. Badonnel, I. Chrisment, "Monitoring and Security for the RPL-based Internet of Things", Doctoral dissertation, University de Lorraine, 2016.
[27] A. Aris, S. F. Oktug, S. Berna Ors Yalcin, "RPL version number attacks: In-depth study", NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, Istanbul, pp. 776-779, 2016.

Authors Profile

Miss. Hiral Patel is currently pursuing her Post graduation in computer engineering from LDRP institute of technology, affiliated under Kadi Sarva Vidyalaya, India. She has completed her bachelor of engineering from Computer Engineering from Shankersinh Vaghela Bapu Institute of Technology (SVBIT) in year 2016. Few of her domains of interest are Internet of Things (IoT), Sensor networks and Cloud computing.

Mr. Hiren Patel is currently working as a Professor and Head in Computer Engineering Department of LDRP-institute of technology and research-Gandhinagar, India. He completed his Ph.D. from National Institute of Technology (NIT), Surat with Cloud computing as the domain of research. He completed his post-graduation from M. S. University, Baroda and graduation from S. P. University, V.V.Nagar. Having more than 15 years of teaching experience, Dr. Patel has many research papers in various conferences & journals of international repute. Few of his main subjects of interest are Computer Programming, Cloud computing, Parallel Processing, Computer Networking and Information Security and block chain technology.

Mrs. Bela Shrimali is currently working as an Assistant Professor in Computer Engineering Department of LDRP-institute of technology and research-Gandhinagar, India. She has completed her Ph.D in Cloud computing domain from C.U. Shah university and masters in computer science and engineering from Government engineering college, Gandhinagar-India. She is having more than 12 years of teaching experience. Ms. Shrimali has presented and published many research papers in various conferences & journals of international/national repute. Few of her main subjects of interest are Cloud computing, Wireless sensor networks and Blockchain technology.

