International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Assessment of the Various Techniques and Models Used To Secure the Applications of Internet of Things

Manu Raj Moudgil, Anil Kumar Lamba, Er.Priya Gupta

Abstract: ***In The Today's Environment Digitization Plays A Vital Role In Daily Aspects Of Life And Mostly All The Appliances Are Digitally Connected And Smart In Operation That Grows Rapidly In All Over The World. For This, Iot Frameworks Is Mainly Applied And Utilized To Build Different Types Iot Applications. During The Formation Of Applications In Iot, Different Types Of Rules, Standards And Procedures Are Used Which Is Embedded In The Iot Framework. While Implementing The Privacy And Security In The Applications Needs A Variety Of Procedures And Mechanisms For Confirmations That All The Things Are Properly Working And Threat Avoidance. This Paper Focuses On Assessment Of Various Security Mechanisms Which Can Be Applied To Build An Iot Application. Also, The Pros And Cons Of Each Technique In The Domain Of Iot Application.***

Keywords: ***Internet Of Things, Security Architecture, Security Mechanism***

I. INTRODUCTION

In the today's lives from small applications to large systems, IoT (Internet of things) is the key who is powerfully mapped various applications with different domains and framework. IoT describes the role and impact on various applications which are used in our daily life that includes Healthcare, communications and industry environments. Currently mostly daily activities and people interaction with the environment surroundings is confirmed with IoT enrolment. Due to this reason, it is very important to get IoT applications secure and also the ensure the security and privacy for the users is very essential. From the result of need and importance of these applications, we can understand the environment and the challenges of IoT, so that these applications can be easily used and free from mistakes and threats. Generally, IoT applications are written in different programming languages and used many protocols that creates a lot of difficulties and challenges.
So, to avoid such things and issues and requires a good mechanism of security that prevents it from attacks and threats which may can occur.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
Dr.Manu Raj Moudgil*, Professor, department of Computer Science & Engineering, Chandigarh Group of Colleges, Technical Campus, Jhanjeri, Mohali. (Punjab).
Dr.Anil Kumar Lamba, Professor & Head, department of Computer Science & Engineering, Chandigarh Group of Colleges, Technical Campus, Jhanjeri, Mohali(Punjab).
Er.Priya Gupta, Assistant Professor, department of Computer science and engineering, Aryabhatta Group of Institutions, Barnala (Punjab).

This paper flows in such a manner: Section-II Describes the IoT architecture and IoT applications characteristics. Section-III demonstrates the key IoT challenges of security application. Section-IV Describes the recent framework of security in IoT applications. Section-V emphases on the proposed model to secure IoT applications and accomplishes research.

II. PRESENT IOT AND ITS STATE OF ART

The (IoT) Internet of Things is very promising field, that manages a extensive amount of Unavoidable and heterogeneous things with various relating and capacities, those are away from the diverse interpretations through the world [1] [8].

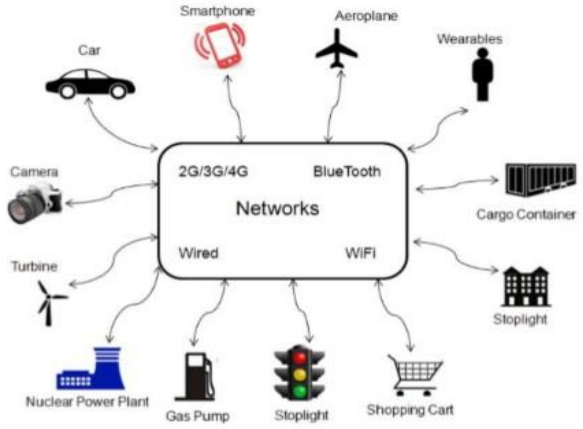

Figure 1: IoT (Internet of Things) [4]

Figure1 Shows that communication gateways which are used to connect heterogeneous devices with the IoT applications. In the decent variety of regions, the significant applications are ready by the IoT innovations which includes, for example security, transportation, medicinal services, industry and observation. Moreover, it has the capacity also to organize advances. For example, Autonomic systems administration, Machine to Machine(M-M) propelled correspondence, Basic leadership, security and secrecy insurance, activation advances and cutting-edge identification with distributed computing. Actually, in the physical world both the dynamic and the static objects are included in IoT and the virtual world which can be coordinated and recognized into communication systems.

The IoT basic includes the followings: (a) Inter-Connectivity,

(b) Administrations things-related which includes for example semantic consistency and security assurance, (c) Heterogeneity, (d) Support for quality of gadgets and the state of dynamic changes, (e) Tremendous scale.[3][8][9]

(A) IoT Architecture:

Generally, IoT applications are formed with the layers set, and with each layer has its own characteristics and attributes that works collectively for achieving the exact goal. The number of specialists worked on internet that is shown in [10][12] which have multiple names and consists of three layers for example layers of network, layers of perception, layer of application and the security problems with each layer. The basic structure and design of internet objects of third layer is shown in Figure2.

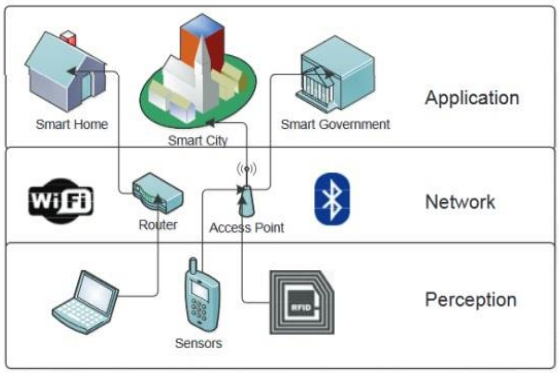

Figure 2: Architecture and Design of IoT third layer [5]

(B) Internet of Things (IoT) Characteristics

IoT have many characteristics which include the following assets:

- **Smart Sensing:** In the IoT all the gadgets having abilities of detection. For example, to turn on and off lights with the utilization of movement sensors. In innovation detection makes the easy understanding and familiarity with the individuals, articles and physical world.
- **Inter-Connected:** For the gadget to gadget interaction it encourages to the users to participate in it.
- **SpareEnergy:** Movement finders are fabricated like motion sensors which are IoT gadgets that can turn on the light when it senses development which can generate some energy from the lift vitality and wastage and also the energy from productive usage.
- **Communicating**: In this the gadget area which is encompasses present state and some associated gadgets, IoT is responsible to advise them. It always inspires machines and humans with better streams correspondence.
- **Intelligence:** In the IoT associated gadgets, knowledge is always attached with them. For example, Wi-Fi authorized Net Learning Thermostats.

III. IOT CHALLENGES OF SECURITY:

The main focus of the IoT (Internet of things) associated gadgets is on security. The information of IoT application can be very close to venture, home, customer or mechanical and also secure the information from altering, robbery and be ensure in the travelling and still. Such as, the application of IoT can stores and recorded the information of the user wellbeing, area, shopping conduct, business orders and amount of stock etc. The IoT strengthen next level of outsourcing. Though, there are doubts around adaptability, accessibility, reaction time, protected innovation possession and value structure and so on. In the time being, numerous difficulties are obstructing the IoT. Concerning versatility, the IoT applications which requires vast quantity of gadgets are often very difficult to execute as a consequence of the detentions on memory, preparing, time, and limitations. For example, large number of gadgets are required to estimate the temperature of everyday as it varies from nation to nation and result of measurement is unmanageable. Also, the equipment which is sent in IoT have varied working qualities. For example, Blunder Dispersions and examining rates, after that the actuators and sensors IoT Parts are constantly remarkably overwhelming. These types of components are compiling to run the IoT varied systems in the IoT information is heterogeneous. Also, it is very difficult and costly to transmit the large volume of unstructured information in a heterogeneous and unpredictable system, So IoT needs information combination and information pressure to reduce the volume. Thus, information institutionalization handling for the IoT future is remarkably needed.

When the information is processed over the internet or even privacy systems, security is prime concern. For example, Government controls health insurance portability and HIPA Act(accountability) on transporting the information over globe can be associated as wellbeing actions. The key security of IoT guarantees that the application assurances like DDoS (Distributed Denial of Service) are setup. When the character of elements asks an access to information by showing multilevel confirmation, it checks and fuse the measures.[13][14]

- **Information Security:** The IoT (Internet of things) information is enabled to exchange from the gadgets consistently over the internet from the observation gadgets. In all the cases information security is test here to make is secure and reliable.
- **Information Privacy:** Smart TV assembles information about study tendencies and for some cases, they listened discussions back to marker.
- **Technical concerns:** Every gadget of IoT can measure the gigantic of information. It is test to Breakdown, Secure and store. That system having an ability to deal with the thickness and high volume of the gadgets. Moreover,

it lies to fit between the separate and distinguish and the rebel gadgets.

- **Insurance Concerns:** The concerns of the protection industry are about the independent autos. However, by the information it is very easier to evaluate the dangers and also gives chance for valuing new models. For example, driving information and the Wellbeing turning of light protection premium.
- **Legal and Social Concerns:** To address the legal and social concerns, there is no such type of instrument is available.[2]
- Absence of Common Standards: There is absence of the brought together some standards in the IoT and the acknowledgement in the industry to bound together is an enormous test.

Furthermore, Protocols for the preserving-privacy for reliable and secure aggregation of the data in the IoT Enabled Metering smart systems explained by Samet Tonyali.et.al.[17]. This paper describes the issues of the protection which is raised by the savvy metering frameworks to visit information. Recent frameworks, apply the protection scheme by deleting information which in in-organize. (MPC) [15]. For that both the MPC secure and FHE delivering range in the situations of IoT. For this, SametTonyali, et.al. projected a new convention that uses both secures MPC and FHE in the SG (Smart Grid) AMI (Advanced Metering infrastructure) to reduce the overheads during the practical protection and safe guarding information component.

The idea of Internet of Things and its attributes clarified by the Singh et al. [4] and also, he clarifies innovation selection patterns, security challenges and endorses plan for E-commerce enterprise.

The security problems that portend the solicitations of Internet of Things as they rely deeply on the Internet, this study was proposed by the Jing et al. [18]. And also, in detail discuss the three layers of internet of things. The First: layer of application, the second: the layer of observation and the last: the layer of data transfer. In the defined research, stress was given on the problems related to security of every layer in particular. Also, it provides answers to the problems of heterogeneity in full detail by learning all the issues related to security that belongs to internet of things in broad terms. In the last this paper also gave information about issues of security in internet of things and predictable systems and introductory issues of security in internet of things.

How to connect the objects altogether, how to connect anything to anything else, Mahmoud et al. [5] showed and examination and also a related study for the concept of Internet of Things system. Three layers defined by him in the architecture of internet of things , First is : the layer of visualization , Second is: layer of network and the third is: the layer of application that helps in adopting the fix set of standards for the security issues that attain the actual levels of security in every layer and to attain a rich level of security for applications of internet in broad terms. Numerous Information technology professional have functioned on several problems related to security in several internet classes by applying and executing counter measures and actions against these assaults and risks belonged to security. In order to provide the full protection, all security principles, procedures and challenges were identified.

IV. PRESENT CONTEXTS & ARCHITECTURE OF INTERNET OF THINGS SECURITY TOOL:

Trust Aware Access Control System for IOT (TACIoT): A multi core system is a system that relies on more than one standard or factor and trusts seriously on constructing Internet frame-work of things. How to achieve maximum levels of security challenges, the internet of things is still functioning on this to builds mechanism in relation to the same. In the last few years a no. of works & initiatives has been commenced to design and build the services and models within precise vision. To meet a variety of necessities, regardless of nature of internet applications, the vision has been designed and built within the precise domains. A initiative has been built in this sense names as The FP7IOT: This works on the interoperability system among the several applications of the internet to make a world-wide system of services under the roof of public frame-work for a list of applications.

This scheme is the allusion model called Acorn RISC Machine. This Scheme is depended on the preferment of a joint meaning & understanding of rich level of thought by telling the organizational arrangement of internet applications called IOT-A. Several add-on initiatives arose as the starting point of designing a combined security system through this system, such as Bulter and the acceptance of such schemes on the basis of credentials of suitable security and confidentiality mechanism for internet situations that led to several of the privacy issues achieved for applications. Fig. 3 demonstrates several functions of protections inside this model.

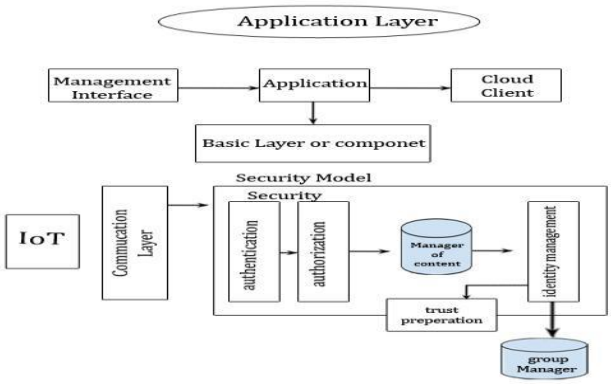

Figure 3: Internet of Things Access Control

The organization of internet uses is sustained by the development and design of precise mechanism to build and deploy regular solutions for the security with the heterogeneous medical thought which is implemented by the internet applications.

The constrained application protocol is the security infrastructure protocol that came under the mostly used and important protocol that works as a regular transfer of discretion in internet object scenarios. The HTTP standards are just same as COAP protocol, all of the services can be performed by all on the networks and also on restricted devices. By connecting security layer to the datagram, it provides several security modes for protocols.

Maximum of the investigation and the scientific research community in current times has acknowledged countless consideration in the usage of access control mechanisms and began many efforts to appear in this direction and also the control of the internet of things.Though, because of many of the limitations on internet h/w resources, maximum of the suggestions accepts the use of crucial entity on the internet, accountable for access control and security mechanisms.

Due to this, the lack of a suitable internet access control resolution, the Internet Engineering Task Force (IETF) working Group for approval and authorization of restricted environments (ACE) was designed a regular licensing and authentication mechanism that are positioned on networks and devices with partial resource constraints.

V. PROPOSED METHODOLOGY:

ACCESS CONTROL CONTEXT FOR INTERNET OF THINGS DEVICES:

Access control context for internet of things (IOT) devices & their services, through security guidelines placed on resource rich infrastructure nodes.

The Created Oauth–Internet of Things structure proposes to get control systems for the Internet of Things, by suitably applying and fitting the normally operated exposed bench-marks. The reference engineering holds the supplementary divisions:

1. **Internet of Things Network:** It includes abundant appreciative devices prepared to perceive the encircling condition secure evidence, (e.g. temperature, stickiness, ruddiness, and rushing) and send them to a basin hub, moreover called organize organizer, through a very less power and small remote communication invention. The basin hub is joined to the Entryway that goes about as a resource Server and offers much helpfulness.
2. **Gateway:** It is a important centre of the planned engineering that implements the OAuth-2.0 Resource Server and a line between Outh-2.0 and the I.E.T.F. resolution stack. For certain, it proposes security functionalities (for example basis of Transport Layer Security station with the customer, access control & verification), the following of accessible assets (through the asset exposure method), and other context functionalities (e.g., info storage and cleanliness controls).
3. **Client:** In agreement with the Industry Standard protocol for authorization OAuth-2.0 approval structure, it is an outsider submission eager to attain assets taking a place with an Internet of Things position, for the asset owner. It would get to faraway assets through standard protocol OAuth-2.0 natives.
4. **Authorization Server:**It achieves endorsement mechanisms, as given by the OAuth-2.0 authorization contexts.

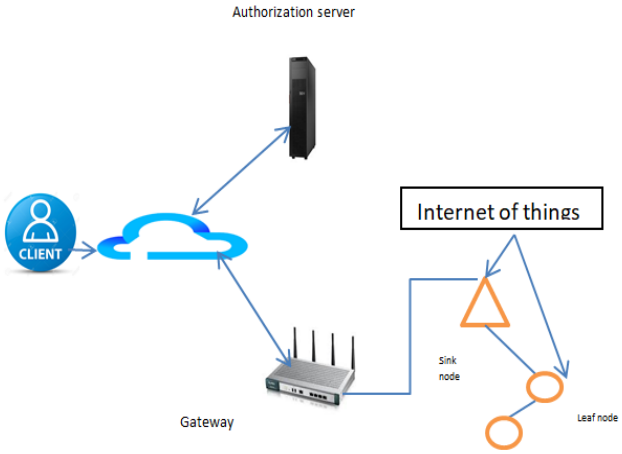

Figure 4: The proposed architecture Oauth-IoT Framework

(A) Use Internet of Things Data Encryption:

To defend the confidentiality of users and stop Internet of Things data breaks, encode the data at break and in-transit among Internet of Things devices and back-end systems by using regular cryptographic procedures and completely encoded key life-cycle organization procedures to increase the complete security of user facts and confidentiality.

(B) Use of Internet of Things Application Program Interface Security Methods

Use of Internet of Things Application Program Interface Security Methods not only to defend the truthfulness of the facts crusade among Internet of Things devices, backend systems, & submissions using familiar REST-based A.P.I's, but also to safeguard that only legal devices, apps & developers are collaborating with A.P.I's or distinguishing probable threats and assaults in contradiction of precise A.P.I's.

Table 1. Summary of different security mechanisms used for securing IoT applications

Methods	Limitations	Advantages	References
The Constrained Application Protocol (COAP)	Lack of an appropriate Internet access control solution.	It provides many security modes for protocols by connecting the security layer to the Datagram	[7] [9] [10]
Trust Aware Control Internet of Things: This model builds domains to meet a range of requirements.	Trust Aware Control -Internet of Things (IOT) should be implemented and evaluated in a real test-bed for constrained and non-constrained Internet of Things (IOT) devices.	Trust Aware Control - Internet of Things (IOT) extends traditional access control systems by taking into account trust values which are based on reputation, quality of service Understanding and meaning of a high level of abstraction by describing the structural structure of Internet applications called Internet of Things (IoT)-A. Through this system, a number of additional initiatives emerged as the starting point for designing a unified security system.	[9] [10]
Access Control Framework [OAuth-Internet of Things (IOT)]	OAuth-2.0 focuses only on client developer simplicity while providing specific authorization flows for web applications.	In accordance with the OAuth-2.0 approval structure, it is an outsider application willing to achieve assets having a place with an Internet of Things(IOT) arrange, for the asset proprietor secure information. It incorporates numerous obliged devices ready to detect the encompassing condition.	[4] [5] [9] [10]

VI. RESULT & DISCUSSIONS

This paper discussed about all the different security mechanisms that mainly used to secure IoT applications and we found thatThe Constrained Application Protocol (COAP) has an advantage that it provides many security modes for protocols by connecting the security layer to the Datagram but lack of an appropriate Internet access control solution.Trust Aware Control Internet of Things: This model builds domains to meet a range of requirements, it extends traditional access control systems by taking into account trust values which are based on reputation, quality of service, also the Understanding and meaning of a high level of abstraction by describing the structural structure of Internet applications called Internet of Things.In accordance with the OAuth-2.0 approval structure, it incorporates numerous obliged devices ready to detect the encompassing condition.So, we found thatOauth-IoT Framework is very much beneficial in terms to securing Iot applications as it has all the features which is COAP and Trust aware control method and also it is much easier to implement and provides data encryption for security IoT applications.

Table 2 below shows the overhead which is caused by access control mechanism which is proposed in this paper with different packet sizes. The overhead that is the ticket size is 6 to 10 bytes in normal cases

Table 2 CoAP Normal Message Size Vs CoAP+AAA

	CoAP		CoAP+AA	
	request	response	request	response
GET	N	N	N+T	N
PUT	N	N	N+T	N
POST	N	N	N+T	N
OBSERVE	N	N	N+T	N
DELETE	N	N	N+T	N
ACK	N	N	N	N
RST	N	N	N	N
.well-known/core	N	N	N+T	N
.well-known/ auth?login	-		I	N+T
well-known/ auth?logout	-		O	N

N means Normal size
T means Ticket size
I means Login request size (I>S)
O means Logout request size (O>=S+T)

VII. CONCLUSION

Today Internet is projected to integrate cloud computing, advanced communication technologies, simulation and sensing making a way to all the leading applications in distinct areas which affects the daily aspects and routines of the lives of people and brings numerous amenities. Due to the connected devices which are very large in the number, a lot of risks are also there which targeting the privacy, governance and the security issues over the internet.

This paper has covered all the challenges and security issues on the Internet of things and also grants open challenges in the area of IoT and research. Furthermore, this paper discussed the problems of the IoT applications related to the security and provide some suggestions regarding the solutions which are previously presented. Finally, the assessment of the various tools has been done by the research to determine various levels of security for Internet of things applications and also with some current methods which are proposed, that research should overcome and avoid the limitations in the security methods of IoT by providing the optimal solutions of the security.

REFERENCES

1. Nitti, M., Pilloni, V., Colistra, G., &Atzori, L. (2016). The virtual object as a major element of the internet of things: a survey. IEEE Communications Surveys & Tutorials, 18(2), 1228-1240.
2. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 27872805.
3. Bernabe, J. B., Ramos, J. L. H., & Gomez, A. F. S. (2016). TACIoT: multidimensional trust-aware access control system for the Internet of Things. Soft Computing, 20(5), 1763-1779.
4. Singh, S., & Singh, N. (2015). Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. In Green Computing and Internet of Things (ICGCIoT), International Conference on (pp. 1577-1581). IEEE.
5. Mahmoud, R., Yousuf, T., Aloul, F., &Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures. In Internet Technology and Secured Transactions (ICITST), 10th International Conference for (pp. 336-341). IEEE.
6. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., Qiu, D. (2014). Security of the internet of things: Perspectives and challenges. Wireless Networks, 20, 2481-2501.
7. 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, 2347-2376.
8. Ashton, K. (2009). "That internet of things' thing," RFiD Journal, 22, 97-114.
9. Atzori, L., Iera, A., Morabito, G. (2010). The internet of things: A survey. Computer networks, 54, 2787-2805.
10. [M. Abomhara and G. M. Koien, (2014) "Security and privacy in the Internet of Things: Current status and open issues," in Int'l Conference on Privacy and Security in Mobile Systems (PRISMS), 1-8.
11. K. Zhao and L. Ge,2013 "A survey on the internet of things security," in Int'l Conf. on Computational Intelligence and Security (CIS), 663-667.
12. M. Leo, F. Battisti, M. Carli, and A. Neri, 2014. "A federated architecture approach for Internet of Things security," in Euro Med Telco Conference (EMTC), 1-5.
13. M. Farooq, M. Waseem, A. Khairi, and S. Mazhar,2015 "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Perception, vol. 111.
14. [R. Roman, P. Najera, and J. Lopez, 2011 "Securing the internet of things," Computer, vol. 44, 51-58.
15. R. Roman, J. Zhou, and J. Lopez,2013. "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, 22662279.
16. Romdhani, Imed&Abdmeziem, Riad&Tandjaoui, D. (2015). Architecting the Internet of Things: State of the Art.
17. [SametTonyali, Kemal Akkaya, Nico Saputro, A. SelcukUluagac, Mehrdad Nojoumian, 2018. Privacy-preserving protocols for secure and reliable data aggregation in IoTenabled Smart Metering systems. Future Generation Comp. Syst. 78: 547-557.
18. Qi Jing, Athanasios V, Vasilakos, Jiafu Wan, Jingwei Lu, Dechao Qui,2014 "Security of the Internet of Things: perspectives and challenges", Springer, Wireless Networks, vol. 20, Iss.8, pp. 2481–2501.

AUTHORS PROFILE

Dr.Manu Raj Moudgil, is working as a Professor in the department of Computer Science & Engineering at Chandigarh Group of Colleges, Technical Campus, Jhanjeri,Mohali. (Punjab).He is having rich experience of more than 15 years in teaching of graduate and post graduate classes of Engineering students, also currently guiding and guided many M.Tech thesis and Phd Students for the research work. He has more than 50 quality research publications in International Journals/Conferences and his area of research is Natural Language Processing, Machine translation systems, High level Languages and Computer Networks. Beyond this he has got many awards like Teacher of the Year for the session 2008-09 and 2010-11 for the Excellency in Teaching. He is written a book OOPS paradigm using C++ and some in process He is also awarded excellent research paper many times in the international conferences, recent one in Melbourne, Australia in 2018.

Dr.Anil Kumar Lamba, is working as a Professor & Head in the department of Computer Science & Engineering at Chandigarh Group of Colleges, Technical Campus, Jhanjeri, Mohali(Punjab). He is having rich experience of more than 22 years in teaching of graduate and post graduate classes of Engineering students, also currently guiding and guided many M.Tech thesis and PHD Students for the research work. He has more than 20 quality research publications in International Journals/Conferences and his area of research is Security in mobile adhoc networks, High level Languages. He had written international book on load distribution in peer to peer networks and some more in progress.

Er.Priya Gupta, is working as Assistant Professor in the department of Computer science and engineering at Aryabhatta Group of Institutions, Barnala (Punjab).She is having an experience of three years in teaching of graduate and post graduate classes of engineering students.She has two quality research publications in international journal/conference and her area of research is Cloud computing and big data analytics.Beyond this she got appreciation for best efforts in Teaching.She is written a book on fundamentals of information and technology, C++ and some in process.She is also awarded excellent research paper in the International conference in 2019.