International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Taxonomy towards Security using Encryption Algorithms in IOT-Based Healthcare System

Swati Jaiswal, Lakhan Singh, Supriya Sarkar

Abstract: ***As IOT has emerged itself in multiple domains that allow proper communication and connectivity worldwide. Due to that multiple attacks and threats arises, which creates number of solutions towards the same. It also raises some important questions and challenges for the security of systems, devices and networks. Multiple algorithms have been devised earlier for wired, wireless, and M2M communication which are not feasible for IOT devices due to low battery life and short range devices. The author focuses on detail analysis of various algorithms, encryption techniques used for preventing and avoiding security threats in IOT-based healthcare systems.***

Keywords: encryption, data privacy, security threats, security.

I. INTRODUCTION

The IOT has not been around for very long. In early 1800s there have been visions for using machine for communication from one another. It provided direct communication since the first landline was developed in 1840s. Then an era of wireless telegraphy took place in 1900. After that in 1950 the use of computer became started and internet became the significant component of IOT. In 1999, Kevin Ashton, the executive director of Auto ID labs at MIT emerges the concept of IOT in his speech and believed that RFID is requisite for using IOT for communication. By the year 2013 IOT boomed internet market and almost covers all domain whether it is embedded system, wireless communication, electrical system (smart grid, smart meter) and machine communication. It allows multiple devices to interconnect through the internet and makes user time more productive [1]. For example, consider a situation where your printer has low pages and it can automatically order pages through internet or your wearable devices inform you when and where a person can utilize his time most effectively. This is possible by the implementation of IOT. Google echo dot and alexa are one of the best examples that provides ample of information like weather forecast, traffic congestion, daily news, appointments, read mails, current affairs and it can also provide entertainment. The IOT provided innumerable options to intercommunicate devices and equipments. IOT can be a used in any communication like smart home, smart city, smart industry, smart meter, smart industry etc. Nowadays, IOT has become the key aspects of healthcare management system. The amalgamation of IOT with healthcare has become the new revolution towards medical science in real time system. Ubiquitous health monitoring provides circumstantial information about old age and ill patients.

Continuous monitoring and prior response to medical situation not only leads to increase the life of patient but it also allows families to provide better healthcare to their kids and elderly people[2]. For implementing IOT based healthcare system biosensors, RFID based IOT distributed architecture, wearable devices and mobile IOT applications can be used. As the evolution of IOT provided new wings to the society it also imposes certain challenges also[3]. As the advancement IOT in healthcare increases it also attracts various challenges towards security and privacy issues. Sensors and video cameras capture information from public areas and store the same in local or cloud based storages. These days the customers are forced to surrender their privacy for the sake of information. Hence security, privacy, data sharing and trust management should not be taken lightly, as it imposes a lot of risk towards the usage of IOT [4]. Significantly a number of studies have been done on providing security to IOT based healthcare system.

The literature shows some problem against security and their significant solutions in different areas like health care monitoring and management of data for kids, adults and elderly people using different cryptographic techniques. Hence the following contributions have been summarized in this paper [5]:-

1. Represents various states-of-art for existing privacy and data integrity techniques.
2. It provides classification and uses of different cryptographic techniques.
3. It highlights future work for achieving essential security systems.

II. TAXONOMY OF STUDY

As IOT expanded their wings in different domains in society it requires the amalgamation of sensors with cloud computing technologies for storage, access and management purpose. The use of S-CI in healthcare allows various cryptographic techniques to be efficiently implemented for IOT as shown in fig1. Some of them are discussed below:

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
Swati Jaiswal*, Department of CSE, VIT, vellore, India. swatijaiswal26@gmail.com
Lakhan Sisodiya, Department of CSE, Medicaps Institute of Science & Technology, Indore, India.sisodiya.lakhan53@gmail.com
Supriya Sarkar, Department of CSE, VIT, vellore, India. supriya.sarkar@rediffmail.com

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

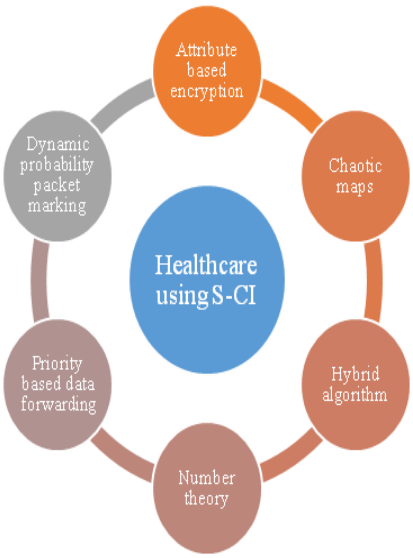

Figure 1: S-CI based algorithm

a. Chaotic maps [6], in 2016, author proposed framework for continuous monitoring of patients data with use of chaotic map security system. The problem with existing system was the data passes through public and insecure communication channel. The idea to design such algorithms is to achieve data privacy and security of sensor data in cloud structure. The first step to access this system is to register itself to trusted cloud system to get chebyshev chaotic map-based certificates. When any patient visited to health care centre, doctor and patient upload medical report to cloud centre. The data will be available in cloud whenever it is required by trusted authority. In case of emergency, the medical caregiver directly access cloud centre data of patient and treat them without wasting anytime. This helps patient and their family to closely monitor and manage chronic diseases effectively.

It makes difficult for an attacker to crack secret parameter based certificate as it is only known to the concerned ones. But the average communication cost is not evaluated properly.

b. Hybrid algorithm [6], as the name suggests this cryptographic technique makes use of both symmetric and asymmetric encryption techniques. Author explained sensor and cloud based computing based secure IOT scheme for elderly patients using mobile applications/devices. Before initiating medical process, both medical officer and patient need to register in key generation centre via secured channel. It helps to create secure communication channel among patient and caregiver.

After visit the medical report will be uploaded to cloud by medical staff officer and also the same report with test evaluations is uploaded by patient using mobile device. On server end, the received data is compared to the standard values which are already stored in the database for proper evaluation. After comparison, if the received data values are greater than stored standard values it means emergency condition arises and same should be inform to emergency family contact. Otherwise the report is provided to patient mobile device. For the same it uses double layer encryption technique for different layers of security like for data collection and storage level it uses confidentiality and integrity measures, for data transmission over network it uses security and confidentiality and for accessing stored data it uses authentication and authorization.

In Hybrid algorithm, symmetric encryption is used because of its efficiency as the same key is used for encryption and decryption process. Whereas, asymmetric encryption is used due to its public, private key structure and easy to use its distribution during transmission [5]. The advantage is it reduces wastage of medical resources and provides better security. But it is difficult for elderly people to use and more computation is required.

c. Attribute based encryption-for achieving security in IOT communication, ample of algorithms are been designed using ABE. In 2015, a Mask-certificate ABE has been introduced for secure data transfer. The main aim of this study is to achieve privacy and access control for secure transfer and storage of PPPs data. It consists of seven algorithms like setup, key generation, certificate generation, encryption (DO and ESP) and decryption.

Then in 2016, author expanded its own algorithm into another scheme for secure access control. It makes use of mobile based data collection using S-CI in bulk. It performs masking of plaintext using specific signature systems and also performs authorization. The scheme was convenient, easy to compute and has less storage cost. Afterwards in 2017, a new mechanism based on mobile healthcare social networks (MHSN) introduces which also uses ABE and identity based encryption scheme. The main focus of algorithm is data privacy and security of patient's data and social data together with proper access control as depicted in Table1. It makes use of independent algorithm for encryption and decryption of data. With that it show more efficient and secure algorithm than other schemes.

Table1: Variations of ABE in healthcare

Algorithms	Achieved	Controlled By	Emergency management	Limitations
ABE Scheme	Avoid unauthorized access control	Third-party trusted authority	None	Do not provide security with access control
MC-ABE	Secure transfer and storage of data, also achieved access control and data privacy	Data owner	None	Need to improvise scalability
Extended MC-ABE	Fine access control	trusted authority	None	Real access of patients data is not available
MHSN	Data privacy is good	trusted authority	None	Storage cost is not calculated

d. Gope-2016 uses BSN –care (Bio-sensor network) for healthcare system. BSN is an intelligent and low power consuming sensor nodes that can be used on or around human body. The use of BSN can provide all the information and report by monitoring human body. BSN system uses two types of sensors in-body and on-body. The in-body sensors allow communication between implanted sensors and base station whereas on-body sensors can provide communication between wearable devices and their coordinators. The BSN architecture consists of invasive and non-invasive devices.

Multiple type of sensors are integrated with bio-sensors for gathering physiological parameters like ECG, EMG, and BP etc from human body. These parameters are passed to a coordinator called as local processing unit (LPU). LPU can be any hand held devices like smart-phone PDA etc. It works as a router between BSN nodes and server system. When any kind of abnormality can be detected in bio-sensors implanted human body, LPU informs the same to the person who uses wearable devices and also the same information can be stored in server. The server keeps update the database and analyses the data the stored data to find abnormalities. If the degree of abnormalities goes high, it informs to family member of patient or nearby physician.

For proper working of this scheme some parameters have been used known as family response (FR), physician response (PR) and emergency response (ER). Author uses Boolean variables true or false for representing the condition and action against the same. Table 2 represents data monitored from patient and action taken.

Table2: Data monitored from patients

Data capture through sensor (BP)	Condition	Action taken	Response against action
BP≤120	-	No problem	Not required
BP>140	Not serious	Inform to FR	FR:True/False
BP>180 && FR=F	Serious	Inform to PR	PR:True/False
BP>180 && PR=F &&TR=F	Emergency required	INFORM to ER	ER:True/False

BSN-care scheme will provide greater help to monitor old age people and patients at home.

One question arises that how this algorithm i.e. BSN-Care achieves security? For answering the same author introduces lightweight anonymous authentication protocol. Protocol basically works on two phases in which phase 1 explains about registration process and phase 2 defines anonymous authentication phase. Phase 2 provides end to end security i.e. BSN server and LPU will authenticate each other before communication. By using this protocol the author achieves mutual authentication, anonymity and secure localization property. It also helps to reduce computation overhead and defeat replay attempt.

e. The author proposes an anonymous authentication scheme which ensures sensor untraceability, anonymity, resistance against replay and clone attacks. This scheme applied over distributed IOT system architecture [15]. Distributed architecture contains four components like authenticated cloud server (ACS), cluster-head (CH), home IOT server (HIOTS) and sensor node.

- Sensor nodes- these are edge devices which can move from one network to the other for information gathering.
- Cluster-Head- CH are the relay devices which conveys the sensor encoded data to HIOTS. CH also verifies the authentication of sensor nodes to HIOTS.
- HIOTS- HIOTS works as gateways and are responsible for the authentication of sensor node. HIOTS verifies the originality of sensor nodes. It also checks whether sensor node can enter CH or not.

The communication of devices involves following steps:

1. Firstly all the CH and sensor nodes need to register themselves to HIOTS.
2. Then HIOTS will send back security credentials to the registered devices.
3. In next step HIOT will register itself to ACS. ACS allows the interaction of two HIOTS.
4. If user wants to access some real time data from sensor node, which is available at HIOTS, then HIOTS server need to register users through ACS.
5. When sensor nodes moves from one network to another then current HIOTS checks to find the original HIOTS of moved sensor node to verify its originality.

Applications- It can be used in RFID based distributed system applications where a person having RFID tag sensor can move between building blocks. In that case tag reader worked as CH and backend data server as HIOTS. Another application is health care based distributed system with the help of bio-sensors and mobile- IOT applications.

f. The weave of cloud computing with wireless body area networks has strengthened the attributes like storage, range capabilities, power and management [6]. Chronic patients can be addressed more effectively with information made available through ubiquitous healthcare monitoring. Such information is helpful not only for elderly people but also to the young generation in fighting for chronic diseases. The literature explains patient's physiological parameters i.e. PPP framework for chronological patients as follows:-

a. First find out all the basic requirements (preliminaries)
b. Identify the entities
c. Then select appropriate technique
d. Access patients physiological parameters
e. Perform security analysis
f. Last but not least, calculating system performance.

For providing security in healthcare data management system and electronic healthcare system, S-CI makes use of Attribute based encryption technique. It also uses different algorithms for e-health systems such as multi-valued encryption, tri-mode algorithm, number theory, hybrid encryption, priority based data forwarding and dynamic probability packet marking. Table 3 represent comparison of various cryptographic algorithms used in IOT- based healthcare system.

Table3: Comparison of cryptographic algorithms in healthcare system

Authors	Algorithm implemented	Methods/Solutions	Security Services	Pros	Cons
Wood et al[7]	AES & MAC	ALARM-NET (Query based system)	Authentication using Secure remote protocol	Provide secure end-to-end communication, reduces power consumption and overhead	Highly susceptible to confidentiality attack
Huang Y.M [8]	AES and polynomial based encryption (for point-to-point communication)	Wireless sensor motes with Bluetooth chip	Authentication mechanism for Bluetooth	Low power consumption, prevent replay and impersonation attack	Does not detects chronic patients location
Yanmin et al [9]	Diffie-Hellman and symmetric key algorithm	Finger based policy (event-condition-action mechanism)	Authentication and authorization	Guarantees data integrity	Does not support dynamic code modification
Ko J et al [10]	Data compression algorithm	MEDiSN	Collection tree protocol (CTP)	Protection done by hop-to-hop basis	Need more security measures against attacks
Yu et al [11]	Attribute based encryption	Fine grained distributed access control (FDAC)	SHA-I and AES	Distributed data storage	Due to distributed data storage more security is required
Zhaoyang et al[12]	Hash based and MAC	BAN (plug n play)	Improved jules sudan and key agreement algorithm	Improves data confidentiality, security and data authentication. Low overhead	Vulnerable to Sybil, sinkhole and wormhole attacks
Hu C et al [13]	Fuzzy ABE and Digital signature	FABSC (Based on fuzzy signature and encryption)	Access control and authentication	Error tolerance and resistance against collusion attack	Access control structure not implemented
Chunhua et al [14]	ECC	RFID based health care system	RFID authentication protocol	Guarantee secure communication	Computational and communication cost is high
Gope et al [15]	Authentication protocol	Distributed IOT system	Anonymous authentication scheme	Avoid cloning, replay attack and sensor anonymity	Some of the attack resistance property is not considered
Xinghua et al[16]	Lightweight Authentication protocol	Dolev Yao model (using k-pseudonym)	Lightweight anonymous authentication protocol	Avoid resource consumption, easy to implement and highly efficient	Generation of K-pseudonym poses burden on server
Wrona et al [17]	ABE with symmetric algorithm	Object level protection and cryptographic access control	Cryptographic access control	Used in military applications,objects can be protected end-to-end	Large amount of data is crucial to manage
Amin et al [18]	Hash function based mutual authentication	Health monitoring using AVISPA tool	Session key negotiation protocol	Reduces energy consumption, offers data CIA, resist untraceability attack, offline password guessing attack and impersonation attack	Not implemented in IOT based environment
Prosanto Gope et al [19]	One way hash function, EX-OR operation and offst codebook based encryption	Secure IOT based HCS using LAAP	Lightweight anonymous authentication protocol	Provide data security, privacy, integrity, anonymity and authentication	High communication overhead
Yeh et al [20]	SHA-3,EX-OR and random number generation function	Secure IOT based healthcare system	Lightweight crypto module	Achieve security and system efficiency	High computation cost
Gope at al[21]	SHA-256 and Ex-OR	MAKA Scheme	Mutual authentication and Fair key agreement	Protection against known session key attack, insider attack and forgery attack	Not tested against other attacks
Li et al[22]	Chaotic maps	Secure mobile based WBAN	Security and privacy	Protects patient privacy, difficult to crack certificate and reduces system overheads	Average access time ignored and average communication cost not calculated
Hu. et al[23]	Hybrid encryption technique	Certificate based S-CI	Data Privacy and Security	Used for continuous monitoring of elderly people, emergency mode working	Not easy to use for elderly people, take more calculation time
Li X et al [24]	SHA-I	WBAN	Lightweight single round authentication protocol	Increases system security, resist forgery, DOS, replay and insider attack	Protocol fail to include GPS data

M. Prabhu et al [25]	Private key encryption	E-Health monitoring	Use of Arduino	Provides authentication and addresses privacy and security issues, cost efficient, due to periodic update system works faster for patients, provided scalable and robust end-to-end security	-

Comparison of algorithms provided roadmap of innovative findings and research in healthcare system. Healthcare monitoring needs proper attention in terms of user-friendly applications, effective management of PPPs data, proper access control, emergency support to patients, network and cloud security. It also requires lightweight algorithms with proper security measures to protect data transfer and communication in cloud. Access control, authentication, data privacy are major requirements for implementing a secure and integral algorithm in healthcare system. Use of arduino, beaglebone and raspberry pi has been used for hardware implementation of the IOT with cloud. It shows that use of RFID authentication protocol provided greater secure communication.

III. CONCLUSION

This study has provided a detailed literature review of various algorithms used for avoiding attacks and threats in healthcare system. As the study shows, healthcare management can be managed through mobile-based and e-based healthcare system, it provided a wide scope to the researcher for future work. However this research area lacks in providing better security to IOT communication along with real time implementation, integration of patients data, lack of emergency call, lack of user friendly accessing of data through GUI interface, lack of efficient access control and lack of proper data sharing and management. The literature suggests that all cryptographic schemes are not applicable in all domains of IOT.

Hence an efficient and secure algorithm is required to achieve data access control, integrity, confidentiality. The framework for future work is also discussed.

REFERENCES

1. Swati Jaiswal, Supriya Sarkar, “COT-Evaluation and analysis of various applications with security for cloud & IOT", book chapter published in IGI global, for a book titled”Handbook on Examining Cloud Computing Technologies Through the Internet of Things", available in GOBI (comes under EBSCO) and OASIS library-2018.
2. S. Al-Janabi, I. Al-Shourbaji,M. Shojafar, and S. Shamshirband, “Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications,” *Egyptian Informatics Journal*, vol. 180, no. 2, pp. 113–122, 2016.
3. Swati Jaiswal, Dr. Chandra M,“A survey: Privacy and security to Internet of Things with Cloud Computing”, International Journal of Control Theory and Application, Volume 09, Number 42 ©International Science Press 2016, page no. 487-500.
4. Swati Jaiswal, Dr. Chandra Mohan, “Variations of Lightweight Encryption Algorithms: A Review, Challenges and Solutions”, International Conference on Electronics and telecommunication system 2018 Karpagam college (ICET’S 2018).
5. Isma Masood, Yongli Wang, Ali Daud, Naif Radi Aljohani, Hassan Dawood, “ Towards smart Healthcare: patient data privacy and security in Sensor-Cloud Infrastructure”, Hindawi Wireless communications and mobile computing volume 2018, pages 23, Wiley Nov 2018.
6. P. Jeyadurga, Dr. S. Ebenezar, I. Joshua Selwyn, P. Sinanisha, “Security in Smart Healthcare System: A Comprehensive Survey”, International Journals of Advanced Research in Computer Science and Software Engineering ISSN: 2277-128X (Volume-7, Issue-10)
7. Wood A, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z.He, S. Lin, J. Stankovic, “ALARM-NET: Wireless Sensor Networks for Assisted-Living and Residential Monitoring,” Department of Computer Science, University of Virginia; Charlottesville, VA, USA:2006. Technical Report CS-2006-01.
8. Huang Y.M, M. Y. Hsieh, H. C. Chao, S. H. Hung, and J. H. Park, “Pervasive, Secure Access to a Hierarchical Sensor-Based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks,” IEEE Journal on Selected Areas in Communications, Vol. 27, No. 4, pp.400-411,May 2009.
9. Yanmin Zhu, Sye Loong Keoh, Morris Sloman, and Emil C. Lupu, “A Lightweight Policy System for Body Sensor Networks,” IEEE Transactions on Network and Service Management, Vol. 6, No. 3, pp.137-148, September 2009.
10. Ko.J, J. H. Lim, Y. Chen, R. Musaloiu-E, A. Terzis, G. M. Masson, “MEDiSN: Medical Emergency Detection in Sensor Networks,” ACM Trans. Embed. Comput. Syst. Vol. 10, No. 1, pp. 1–29, 2010.
11. Yu S, K. Ren, and W. Lou, “FDAC: Toward fine-grained distributed data access control in wireless sensor networks,” IEEE Trans. Parallel Distrib. Syst., Vol. 22, No. 4, pp. 673–686, 2011.
12. Zhaoyang Zhang, Honggang Wang, Athanasios V. Vasilakos, and Hua Fang, “ECG-Cryptography and Authentication in Body Area Networks,” IEEE Transactions on Information Technology in Biomedicine, Vol. 16, No. 6, pp.1070-1078, November 2012.
13. Hu C, N. Zhang, H. Li, X. Cheng, and X. Liao, “Body Area network security: A fuzzy attribute-based signcryption scheme,” IEEE J. Select. Areas Commun. (JSAC), Vol. 31, No. 9, pp. 37–46, 2013.
14. Chunhua Jin, Chunxiang Xu, Xiaojun Zhang, Jining Zhao,“A Secure RFID Authentication Protocol for Healthcare Environments Using Elliptic Curve Cryptosystem,” Journal of Medical Systems, Vol. 39, No. 3, pp.1-8, March 2015.
15. Gope P, T. Hwang, “Untraceable Sensor Movement in Distributed IoT Infrastructure,” IEEE Sensors Journal, Vol. 15, No. 9, pp. 5340 – 5348, 2015.
16. Xinghua Li,Hai Liu,Fushan Wei,Weidong Yang,“A Lightweight Anonymous Authentication Protocol Using k-pseudonym Set in Wireless Networks,” IEEE Global Communications Conference (GLOBECOM), pp. 1-6, December 2015.
17. Konrad Wrona , “Securing the Internet of Things A Military Perspective”, NATO Communications and Information Agency The Hague, Netherlands, 2015
18. Amin, Ruhul, SK Hafizul Islam, G. P. Biswas, Muhammad Khurram Khan, and Neeraj Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," Future Generation Computer Systems, 2016.
19. Prosanta Gope, Tzonelih Hwang, “BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network,” IEEE Sensors Journal, Vol. 16, No. 5, pp.1368-1376, 2016.
20. Yeh, Kuo-Hui, "A Secure IoT-based Healthcare System with Body Sensor Networks," IEEE Access, 2016.
21. Gope P, T. Hwang, “Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility network,” IEEE Systems Journal, Vol. 10, No. 4, pp.1370-1379, Dec 2016.
22. Li, X., Peng, J., Kumari, S., Wu, F., Karuppiah, M. and Choo, K.K.R., “An enhanced 1-round authentication protocol for wireless body area networks with user anonymity,” Computers & Electrical Engineering, 2017.
23. H. He, J. Zhang, J. Gu, Y. Hu, and F. Xu, “A fine-grained and lightweight data access control scheme for WSN-integrate cloud computing,” Cluster Computing, vol. 20, no. 2, pp. 1457–1472, 2017.

24. Xiong Li, Jieyao Peng, Saru Kumari, Fan Wu, Marimuthu Karuppiah, Kim-Kwang Raymond Choo, " An enhanced 1-round authentication protocol for wireless body area networks with user anonymity", Computers and Electrical Engineering, ELSEVIER, February 23, 2017
25. M.Prabhu ,G.Seethalakshmi, Gollapudi Anisha," SECURED HEALTHCARE SYSTEM IN IoT**",** International Journal of Pure and Applied Mathematics Volume 118 No. 20 2018, 3239-3244

AUTHORS PROFILE

Swati Jaiswal Completed M.tech from SIRT Bhopal (Gold medal) and B.E from LNCT Bhopal. Have done many publications in international journal and conferences. Also published 4 chapters in IGI globals. Having 7 years of teaching experience in computer science & engineering.S

Lakhan Singh, completed M.tech from Oriental college of Science & Technology Bhopal. Completed B.Tech from TIT Bhopal, India. I have total 5.4 years of teaching experience.

Supriya Sarkar completed M.Tech from RGTU University Bhopal. Completed B.E from CSE in 2009. Have done many publications in international journal and conferences. Also published 4 chapters in IGI globals. Having 5.6 years of teaching experience in computer science & engineering.