Privacy, Confidentiality And Authorization Preserving Rfid System For Toll Application

Mininath K. Nighot[1] , Nilesh P. Bhosle[2], Vikas P. Mapari[3], Dhanashree S. Kulkarni[4]

[1]Professor, DY Patil Colloege of Engineering, Pune, India
[2]Asso. Professor, DY Patil Colloege of Engineering, Pune, India
[3]Asst. Professor, JSPM's Rajarshi Shahu College of Engineering, Pune, India
[4]Research Scholar, GIT Belagavi, Visvesvaraya Technological University, Belagavi, India

Abstract

Radio Frequency Identification (RFID) technology has a huge demand due to its low cost, wireless communication and real time applications in Toll Plaza. Till last decade, RFID systems were used for healthcare, food and agriculture, manufacturing and logistics, retail industry and vehicle management. Now-a-days, they are widely used in applications where personal and confidential data like location, address and bank details need to be shared through the system. While designing RFID systems, privacy and confidentiality of user's information and user's authorization is not considered. The proposed system mainly focuses to preserve user's credentials from the unauthorized users in tolling system. A box is designed to protect the RFID tag where confidential information is stored. The Box has been designed in such a way that radio waves will not pass in the box. Tag need to be kept in the box when not required. And whenever the user has to give his credentials which are stored on tag, it is required to pull out the tag manually from the box. The rest of the time RFID tag is protected in the box / cover through which any RFID reader will not be able to access it. Hence proposed technique preserves privacy, confidentiality and authorization policies of the user.

Keywords: *RFID, Privacy, Confidentiality, Authorization, Toll Plaza*

1. Introduction

Radio Frequency Identification (RFID) Systems is gaining more popularity due to its day to day real time applications like item level inventory tracking, library systems, real time location systems, attendance tracking, tolling etc.

The RFID system comprises of RFID readers, RFID *tag* and Antennas. RFID *tag* contains an integrated circuit & antenna which is used to transmit data to an RFID reader through the RFID reader's antenna by means of radio waves or electromagnetic waves which is shown in figure 1. Figure 2 shows a block diagram of RFID *tag*. It is a silicon microchip on which antenna, power generator, modulator, demodulator, control logic and memory are mounted. *The tag antenna* receives and transmits the signals to and from the *reader.* Power generator activates the *tag* after first receiving signal from *a reader*. Modulator and demodulator are used to modulate and demodulate the signals respectively. *Tag* information/user's information is stored in the memory. Control logic decides when to send information and which information needs to be sent from *tag* memory to *the reader*.

An RFID *reader* constantly sends radio waves to search RFID *tag*s. Once the RFID *tag* is in the range of an RFID reader, antenna of the *tag* generates power and activates the *tag* system using electromagnetic waves. *Tag* antenna sends acknowledgement signal to *reader* antenna. Now *reader* gets information that *tag* is in the range, so it sends commands to the *tag* to obtain data which is embedded in the *tag* memory. At the *tag* end, once a command is received, *tag* antenna sends the essential details to the *reader* in the encoded form through their antennas. *Reader* decodes the information and sends it to Microcontroller or computer system for processing. Once *reader* receives the information, the vehicle is allowed to pass from toll booth by giving green signal. Then the amount is deducted from an account and user gets acknowledgement of deducted amount. The communication between the RFID reader and an RFID tag is shown in figure 3.

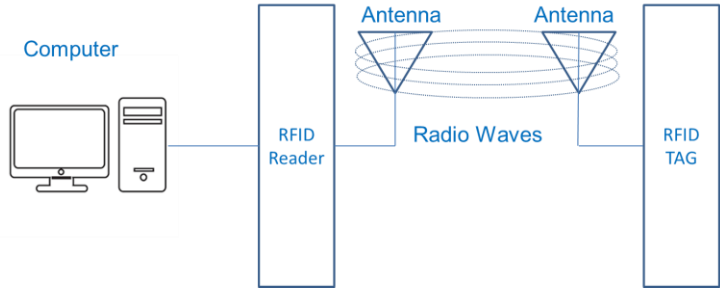

Figure 1: RFID System Setup

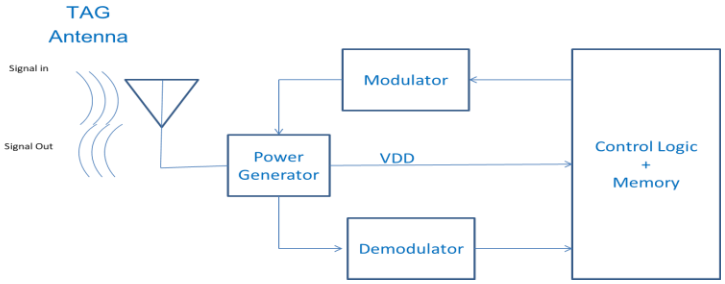

Figure 2: RFID *tag* Block Diagram

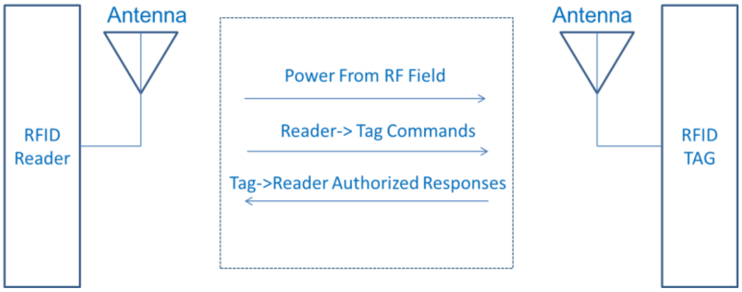

Figure 3: RFID *reader* and *tag* Communication

After receiving information from *tag*, *reader*, *then* decodes the encoded data using a decoder. Collected information of *tag* will be transmitted to a computer or microcontroller for further processing. RFID technology works on Automatic Identification & Data Technique (AIDC). It automatically identifies objects, collects data about them and enters the same data directly to the computer or micro-controller system with little or no human intervention.

RFID operates in Low Frequency (LF), High Frequency (HF), Ultra High Frequency (UHF), and Super High Frequency (SHF) or microwave frequency (MF). Its characteristics are mentioned in table 1.

2. Literature Review

RFID systems are mainly applicable for monitoring items in the applications like library management, retail industry, health care, smart home security and safety, vehicle management and so on. Marinating the data is very difficult, when numbers of items are increased. Cloud computing has come into existence using which it is possible to maintain data and keep data secured [1]. Mainly clouds are used for processing of information and storing the data.

Freq. Band	Antenna	Free Space Range	Operating freq.	Data Rate	Applications
LF	Induction Coil on ferrite core or flat many turns	<10cm	125-134.3 KHz	Slow	Animal *tag*ging, Car immobilizer, Inventory Control, Vehicle Identification
HF	Induction coil flat 3-9 turns	<1m	13.56MHz	Medium	Smart Cards, Item or case level *tag*ging, Vicinity cards, Garment Tracking
UHF	Single or double Dipole	1-12 m	860-960 MHz	Fast	Pallet or case level *tag*ging, Wal-Mart Mandates, Baggage Tracking, Work in progress tracking
SHF/MF	Single Dipole	Up to 100m	2.45-5.8 GHz	Fast	Automatic vehicle Identification, Auto Toll Roads, Pallet level tracking, Container rail car

Table 1: Characteristics of RFID Frequency Bands

.

There are other alternatives like smart cards, bar codes, voice recognition. But all have their own pros and cons. RFID system is robust, low cost, easy expansion in large scale, etc. But RFID cards/*tag*s are more vulnerable for its privacy and security measures. It is easy to get the information stored on the card/*tag* by the attacker. It is also vulnerable to skimming and relaying attacks [2]. Cloning is possible, as RFID cards/*tag*s emit static identifiers. It is possible to access many cards/*tag*s at a time by maintaining proper distance and simulate them. Most of the researchers used cryptographic text for communication to avoid cloning, but still it is vulnerable by the attackers [3].

Leu et al. [4] reviewed RFID sensor applications and its research fields. Author pointed out the research gaps between in-lab investigations and the practical application scenarios like data leakage while communicating *reader* and *tag*, collisions of data, privacy of *tag* holder's details. Mamilla et al. [5] Proposed a RFID based security for paper leakages in the examination. Examination papers are locked in the RFID based, password protected "Electronically locked box". Once it is opened SMS and mail is sent to authorities with its date and time. Devika et al. [6] implemented RFID based theft detection and vehicle monitoring system using Raspberry Pi. When theft is occurring, the system sends mail and SMS to concerned person. Zhen-YuWu [7] suggested Hill Cypher Hard technique to preserve confidentiality, anti-counterfeiting and user's location privacy. The authors provided a solution to malicious tracking and counterfeiting behaviors of attackers. The authors proposed O-TRAP technique which is a matrix-based authentication protocol to focus on confidentiality and the user's location.

WANG et al. [8] intended technique for low communication and computation load of RFID system. The authors used CRC and PNG technique to control processing load on the system. BAN logic and AVISTA protocols are implemented to provide authentication and secrecy policies.

MaBulter et al. [9] proposed Dynamic Risk Assessment Access Control (DRAAC) for intrusion detection to reduce the access privilege of the system. Tian-Fu Lee et al. [10] implemented Quadratic residues for multiple services to secure communication. It preserved the privacy of users. Kai Bu et al. [11] applied a cloned-*tag* identification protocol for RFID. To determine cloned *tag*s, the broadcast & cloned technique is suggested. It consumes time for processing.

There are some problems with existing RFID based Toll Plaza system. Some of them are mentioned here:

1. Existing RFID system directly withdraws the amount from user's account without user's authorization. If the unauthorized RFID *reader* is trying to access user's *tag* information from any public place like on road, parking, city square, then unauthorized user will get access directly and he can make transaction illegally or he will get confidential information which is stored on *the tag*.
2. If user wants to pay the toll amount by cash or by other medium and not from the RFID tag due to some reason, the existing system does not allow this. Even though the user is paying in cash, RFID system deducts toll amount from a bank account which is stored on the RFID tag. Because there is no provision to block RFID *tag* temporarily so RFID *reader* reads *tag* information and processes the transaction.
3. At the tolling booth, if the vehicle is from the local area (less than 20Km), then the vehicle is exempted from toll amount, but for vehicles where RFID *tag* is attached, RFID *reader* reads *tag* information and processes the transaction.
4. If networking is failed from starting tolling booth to existing tolling booth, then existing RFID system collects toll from both tolling booths. Because the system will not have previous tolling booth's data.

After studying existing literature and current application of RFIDs such as Toll plaza, it is hypothesized that a generic solution is required which will work effectively on users' credential's privacy and confidentiality.

3. Proposed System

For the tolling system, users need to embed personal information and banking information like Name, Address, Vehicle details, Bank account number, bank address etc. on the RFID tag. In the existing RFID system, it is expected that RFID *tag* should be attached to the vehicle's front glass so that RFID *reader* can easily read it. The RFID tag chip is accessible by any RFID *reader*. There is no authentication process involved to verify the authorized RFID *reader*. Hence it is dangerous to use in toll like application where personal data and banking information is shared.

So prevention is better to avoid such attacks. A box/bag cover for the RFID *tag* is proposed to protect the unauthorized *reader*'s access. A box/cover is made up with Aluminum/Copper/ any metal foil. These materials have property to absorb electromagnetic/radio waves. If an RFID tag is enclosed by these materials, then it will not charge by *reader*'s signals and further processing will not perform.

Figure 4 shows RFID *tag* and the box material. The cabinet includes an aluminum foil which is fabricated between 2 layers of fiber, plastic or any such material. The size of the aluminum cabinet is slightly bigger than the RFID *tag* as shown in the figure. The aluminum cabinet includes an eject button which will be used for ejecting the RFID *tag* out of the cabinet so that it can be read by the RFID *reader*. The RFID *tag* can be fixed in the box using a wooden plank or any such material which is shown in Figure 5.

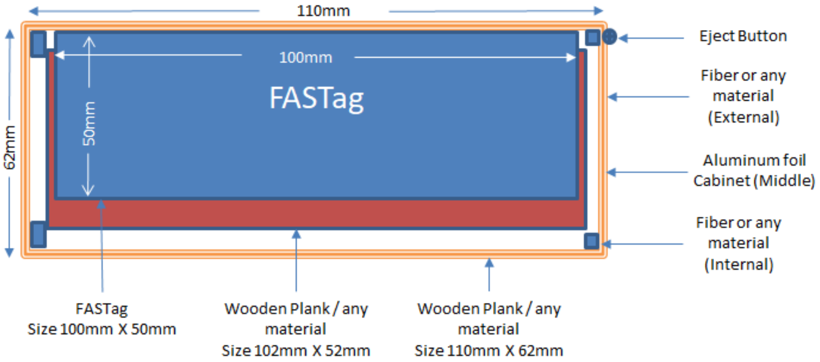
110mm
100mm
FASTag
50mm
62mm
Eject Button
Fiber or any material (External)
Aluminum foil Cabinet (Middle)
Fiber or any material (Internal)
FASTag Size 100mm X 50mm
Wooden Plank / any material Size 102mm X 52mm
Wooden Plank / any material Size 110mm X 62mm

Figure 4: RFID *tag* and Box Material

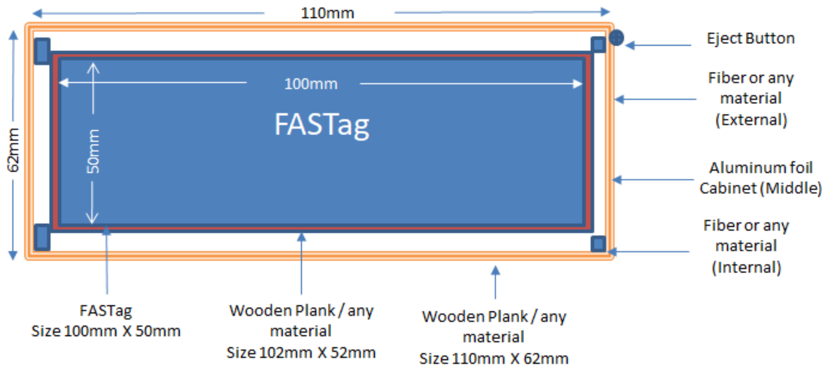
110mm
62mm
100mm
50mm
FASTag
Eject Button
Fiber or any material (External)
Aluminum foil Cabinet (Middle)
Fiber or any material (Internal)
FASTag Size 100mm X 50mm
Wooden Plank / any material Size 102mm X 52mm
Wooden Plank / any material Size 110mm X 62mm

Figure 5: RFID *tag* fixed in a Box

Table 2 describes the material and the size of each layer of box and Table 3 explains the dimensions of box, *tag* holder and RFID *tag*.

Layer	**Material**	**Size**
1 (Outer)	Fiber, Wood, Leather, or any metal	1 mm
2 (Middle)	Aluminum Foil, Copper Foil any metal which absorbs radio waves	1 mm
3 (Inner)	Fiber, Wood, Leather, or any metal	1 mm

Table 2: Three layered box:

Box and *tag*	**Size (Length X Width)**
Outer Box	110 mm X 62 mm
tag Holder	102 mm X 52 mm
RFID *tag*	100 mm X 50 mm

Table 3: Dimensions of Box:

The RFID tag can be ejected from the cabinet either horizontally or vertically. Figure 6 and 7 shows the ejection of the RFID *tag* horizontally and vertically respectively. When the press button is pushed, the RFID *tag* which is pasted on the wooden plank gets ejected out of the cabinet and the notches get locked at the end to hold the RFID *tag*. After the RFID *tag* is read by the RFID *reader* it can be again pushed back in the cabinet, and it gets locked.

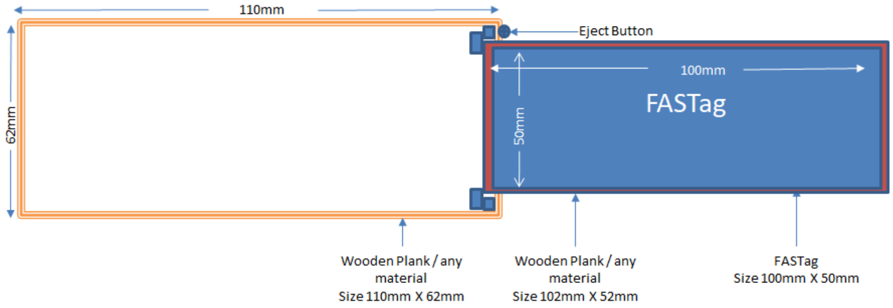
110mm
62mm
Eject Button
100mm
50mm
FASTag
Wooden Plank / any material Size 110mm X 62mm
Wooden Plank / any material Size 102mm X 52mm
FASTag Size 100mm X 50mm

Figure 6: RFID *tag* ejects horizontally to read by RFID *reader*

ISSN: 2233-7857 IJFGCN

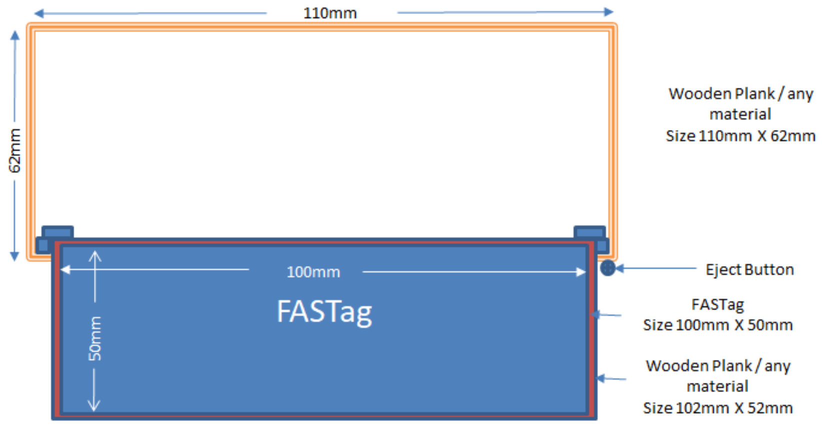

Figure 7: RFID *tag* ejects vertically to read by an RFID reader

4. Results and Discussions

The box is designed in such a way that electromagnetic signals of RFID *reader* will not reach to the *tag* which is fixed into the box which is coated by aluminum foil, copper material or other material which absorbs radio waves efficiently. Due to the box, low frequency electromagnetic waves will not reach to the *tag*, so RFID *reader* will not be able to communicate with *a tag*. Once a user reaches to the toll plaza, it is required to eject *tag* from the box by pressing the eject button. Now *tag* antenna can read the *reader*'s signals and *the tag* will be activated. It transfers necessary information to *the reader*. If the user is allowed to pass the toll, then again user needs to push *tag* into the box. It gives efficient solution of the stated problems.

Table 4 shows the comparison of proposed approach with approaches proposed in the literature with respect to security problems. If the approach has solution to a particular problem then it is represented by "O", otherwise "X". If it is undeterminable situation, we represent it by "△".

1. Whenever the vehicle is either on the road, parking, city square, etc., any unauthorized RFID *reader* can't access the *tag*, if *tag* is in the box.
2. If user wants to pay the toll amount by cash or by other medium and not from the RFID tag, then *the reader* will not be able to access *tag*, as it is in the box.
3. Keeping *tag* in the box, local vehicles (less than 20Km), can pass the toll by just showing valid address proof.
4. It also works if networking is failed on any end or both ends (entering and exiting road) toll plaza.

Problem Approach	**Individual Security**	**Traceability**	**Theft**	**Physical Attacks**	**Counterfeiting**
Jules et al. [12]	O	O	X	Δ	X
Ohkubo et al. [13]	O	O	X	X	X
Inoue & Yasuura [14]	O	O	X	X	X
Proposed Approach	O	O	O	O	O

Table 4: Comparison of RFID security problems

So the said technique protects the confidential information of users from the unauthorized user and avoids unnecessary transactions, hence it preserves the privacy and confidentiality of user's information.

5. Conclusion and Future Work

Mostly RFID systems are appropriate in applications where accessing of data from *tag* is not personal and confidential. The tolling application uses user's personal information and banking information. So there is risk of sharing information with unauthorized user/RFID *reader*. Proposed solution protects RFID *tag* from unauthorized users/ RFID *reader*. Whenever authorized RFID *reader*/user is requesting information which is stored in the RFID tag, it will be accessible by opening cover box/bag in which RFID *tag* is protected. The rest of the time RFID *tag* is protected in the box / cover through which any (authorized/unauthorized) RFID *reader* will not be able to access it hence user's privacy and confidentiality is preserved.

In RFID systems, it is possible to have multiple transactions on the same toll plaza, and needs user authentication for especially banking transactions. In the future, these challenges will be focused to find an efficient solution.

References

[1] S. Jamal, A. Omer, A.S. Qureshi, "Cloud Computing Solution and Services for RFID Based Supply Chain Management", Advances in Internet of Things, Vol. 3 No. 4, pp. 1-7, 2013.

[2] T.S. Heydt-Benjamin, D.V. Bailey, K. Fu, A. Juels, T.O. Hare. "Financial Cryptography and Data Security", IFCA/Springer-Verlag Berlin Heidelberg, USA, pp.2-14 2007.

[3] J. Westhues "Hacking the prox card", Springer, USA, pp.291-300. (2005).

[4] Lei Cui, Zonghua Zhang, Nan Gao, Zhaozong Meng and Zhen Li, "Radio Frequency Identification and Sensing Techniques and Their Applications—A Review of the State-of-the-Art", Sensors, 19, 4012; doi:10.3390/s19184012, 2019.

[5] Mamilla Sirisha, Neelam Syamala, "RFID Based Security forExam Paper Leakage System", International Journal of Engineering & Technology, pp. 841-842, 2018.

[6] P. Devika, V.Prashanthi, G.Vijay Kanth, J Thirupathi, "RFID Based Theft Detection and Vehicle Monitoring System using Cloud", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-4, pp. 773-739, February 2019.

[7] Zhen-YuWu, "An radio-frequency identification security authentication mechanism for Internet of things applications", International Journal of Distributed Sensor Networks, 2019, Vol. 15(7), DOI: 10.1177/1550147719862223, PP 1-10, 2019.

[8] Liangmin WANG, Xiaoluo YI, Chao LV, Yuanbo GUO, "Security Improvement in Authentication Protocol for Gen-2 Based RFID System", 2011 Journal of Convergence Information Technology, Volume 6, Number 1, pp. 157 to 169. January 2011.

[9] Matthew Butler, Peter J. Hawrylak and John Hale, "Graceful Privilege Reduction in RFID Security" , 2011 CSIIRW Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, Article No. 47, pp.47+12, Oct 2012.

[10] Tian-Fu Lee, Hsin-Chang Chen, Pei-Wen Sun, "efficient and secure RFID authentication protocol based on quadratic residues for multiple services", 2010 Computer Symposium (ICS) International conference , pp. 279 – 283, Dec. 2010.

[11] Kai Bu, Xuan Liu, Bin Xiao "Fast Cloned-*tag* Identification Protocols for Large-Scale RFID Systems", 2012 IEEE 20th International Workshop on Quality of Service (IWQoS), pp. 1 – 4, June 2012.

[12] A. Juels, R. L. Rivest and M. Szydlo, (2003), "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", In V. Atluri, ed. 8th ACM Conference on Computer and Communications Security, pages 103-111. ACM Press, (CCS 2003), October.

[13] M. Ohkubo, K. Suzki and S. Kinoshita, (2003),"Cryptographic Approach to 'Privacy-Friendly' Tags", Nippon Telegraph and Telephone, November.

[14] S. Inoue and H. Yasuura, (2003),"RFID Privacy Using User-controllable Uniqueness", Kyushu University, November.

Author Biography

Dr. Mininath K. Nighot has a vast experience of 18 years in the field of teaching and is currently associated with D. Y. Patil College of Engineering, Pune as a Professor and the Head of the Department in the Department of Computer Engineering since 2018. He received his Ph.D. in Computer Science and Technology from Shree Sant Gadgebaba Amravati University, Amravati in 2017. He received his master's degree in Computer Engineering from Dr. D.Y. Patil College of Engineering, Pune, in 2008. He has completed his graduation in Computer Science and engineering from Babasaheb Naik College of Engineering, Pusad, Amravati in 2002. His research interests include RFID Systems, Information security, Wireless communication, Wireless sensor network, and Optimization techniques. His primary area of interest is Wireless Sensor Networks and Information Security. He has published 20 papers in international and national journals and conferences and 7 patents too.

Dr. Nilesh P. Bhosle received his Ph.D in E & TC Engineering from from Swami Ramanand Teerth Marathwada University Nanded, India, in 2018. He received his B.E. degree in Electronics Engineering and M. Tech. dergree in Electronics Engineering from Shri Guru Gobind Singhji Institute of Engineering and Technology Nanded, Maharashtra, India, in 2003 and 2006 respectively. Currently he is working as an Associate Professor in Electronics & Telecommunication Engineering department at D. Y. Patil University, Ambi, Pune. He has more than 13 years of teaching experience and 1 year industry experience. His primary area of interest is computer vision and machine learning. . He also completed one research project funded by Shri Savitribai Phule Pune University under the University Research Grant Scheme. He has published 12 papers in international and national journals and conferences and published 6 patents

Mr. Vikas P. Mapari is pursuing Ph.D. in Computer Science and Engineering from Dr. A.P.J Abdul Kalam University, Indore, Madhya Pradesh, India. He received his M.E. degree in Computer Engineering from DYPIET, Pimpri, Pune, Maharashtra, India and B.E. degree in Computer Engineering from AVCOE, Sangamner, Maharashtra, India and, in 2014 and 2007 respectively. Currently he is working as an Assistant Professor in Information Technology department at JSPM's Rajarshi Shahu College of Engineering, Pune. He has more than 12 years of teaching experience. His primary area of interest is Wireless Sensor Networks and machine learning. He has published 07 papers in international and national journals and conferences and published 2 patents

Mrs. Dhanashree S. Kulkarni is Pursuing Ph.D. at Visvesvaraya Technological University, Belgaum, Karnataka India. She received her M.E.and B.E. degree in Computer Engineering from Visvesvaraya Technological University, Belgaum, Karnataka, India in 2010 and 2004 respectively. Currently she is working as full time research scholar at GIT Research Center, Belgaum, Karnataka, India. She has 13 years of teaching experience in academic and industry. Her primary area of research interest is Natural Language Processing, Data Mining, and Artificial Intelligence, RFID Technology, Wireless Sensor Networks, Network Security etc. She has published more than 08 papers in international and national journals and conferences and published 2 patents.