TRUST MANAGEMENT IN P2P SYSTEMS

Vaibhav Naik[1], Vikas Kapre[2], Sujit Mendhe[3], Amol Gangawane[4]

[1]BE, Department of Computer Engineering, ICOER, Maharashtra, India
[2]BE, Department of Computer Engineering, ICOER, Maharashtra, India
[3]BE, Department of Computer Engineering, ICOER, Maharashtra, India
[4]BE, Department of Computer Engineering, ICOER, Maharashtra, India

Abstract

Peers are more likely to get exposed to malicious activities in P2P system due to its open nature, building the trust environment in P2P can mitigate these attacks. This paper is about the implementation of SORT model in peer to peer systems. The SORT model deals with the isolation of malicious and trusted peer in the LAN (Local Area Network). The isolation is done on the basis of the file uploaded by a peer, i.e. if he uploads an infected file in the proximity then the SORT model restricts the download of the infected file and thus protect the other peers from getting affected by the virus. File download is treated as an interaction. On each interaction there is calculation of some trust factor and the values are assigned by the downloader according to his satisfaction. Every peer calculates its own trust values regarding to other peers. These values are need to decide the further interactions in the network. Two types of attacks are mitigated by this model are Service based and Recommendation based. This project mainly deals with the security in the P2P system and acknowledges the peer whether the service he wants to use is clean or infected. This Project is implemented in Advanced JAVA and the MySQL database is used. The MVC architecture is used for building of this project. Peer calculate the trust metrics of each peer in its proximity they does this locally and do not tend to be global.

Keywords: *P2P systems, Trusted Environment, Reputation, Recommendation, Security, Services.*

----------***----------

1. INTRODUCTION

1.1 Existing System

The existing system consist of central server and data server. Firstly the request of client is passed through a central server, the central server verifies the request or query and check if it's valid or not. And if request is valid then the request is sent to the Main Server for Processing. EBay is currently working on this type of system. Communication with a user can provide some information about the peers, but the feedbacks might contain misleading information Central Server is a concept which is use to prevent the malicious attacks or fake request and provides security but in Peer to Peer system there is no server concept which will rectify the malicious activities, so this system is being built which will provide the security from malicious activity [4].
The Existing System also includes P2P system in which there is no guarantee of what files are shared in the Network. There is no mechanism for concluding the item shared is malicious or not.

1.2 Proposed System

The System we are proposing is a mixture of central Server and P2P, but we are totally omitting the concept of Central Server. The Central Server acts as a filter which filters the request coming to the main server we will design a mechanism similar to central server.

The Mechanism will consists of three metrics and it will work as a central server on every peer connected in P2P system. When a peer shares a file in LAN, let's say that he provides a service to other peers and there is no guarantee of the service whether it is harmful to others or not. Here our system is implemented, It checks the Trust information generated previously and then the decision is taken whether to download the file or not. If there are no interactions previously then there is an option of scan which scans the file and tells a user that if it is infected or not.

The System also shows us a graph which displays the Service history of peers present in the P2P networks. The Graph is a graphical representation of the user's activity i.e. what he uploading, what kind of service he's providing. All the history of past days is shown on in the Graph which is provided to the user. The implementation of System is totally done in JAVA and we use MySQL as a Database, In addition to this we are using technologies such as JSP and AJAX for web development i.e. the Front-End of our Project.

2. LITERATURE SURVEY

In paper [1], SORT: A Self ORganizing Trust Model for P2P Systems" Ahmet BurakCan and Bharat Bhargava proposed a system that can actually mitigate attacks in P2P systems which is huge step towards the security in LAN.

In paper [2], "Trust Management in P2P system using SORT model" published by MJRET authors the same as of this paper, "Vaibhav Naik, Amol Gangawane, Sujit Mendhe, and Vikas Kapre" we proposed an idea of SORT by inspired with the paper [1], in that we told the brief working of our project. Means how it will distinguish between peer on what basis and how will it provide the security in the real time environment.

In paper [4], P. Druschel and A. Rowstron. Past: A large-scale, persistent peer-to-peer storage utility. In Proceedings of the 18th ACM Symposium on Operating Systems Principles (SOSP'01), October 2001. Managing the information related to the trust is directly proportional on the structure of the P2P Model. Peers communicate with each other and calculate the metric of trust with respect to other, each metric is different from each other i.e. metric is built by its own view and thus isolating trust and malicious peers.

In paper [5], J. Heidemann, F. Silva, C. Intanagonwiwat, R. Govindan, D. Estrin, and D. Ganesan. Building efficient wireless sensor networks with low-level naming. In Proceedings of the 18th ACM Symposium on Operating Systems Principles (SOSP'01), October 2001.

Metrics parameters include peer's bandwidth, number of shared files, peer behavior (online/offline, session time) and last resource distribution this will result in the approximated conclusion [5].

In paper [6], D.H. McKnight, "Conceptualizing Trust: A Typology and E-Commerce Customer Relationships Model," Proc. 34th Ann. Hawaii Int'l Conf. System Sciences (HICSS), 2001 Evaluation of acquaintance's trustworthiness in the service context, two belief are calculated i.e. integrity belief and competence belief on the basis of information in its service history. Competence belief symbolizes how well an acquaintance satisfy the need of past interaction [6].

3. WORKING OF SYSTEM

When the system is started, initially there are no past interactions in the system about or no file uploads then the system decides to give chance to strangers to communicate with the peers because the first transaction decides or tells about the user whether he is attacker or a normal user. There are three main models in our system and some subordinate model. The Main Model are responsible for all the working of our project and subordinate model helps main model in term of execution and providing data when they require it. The Project is designed using the MVC Architecture which maintains a simplicity in the project.

At first user need to register on the site with their credentials, the site make sure that they enter correct information because different validation are assigned to it. After the successful registration user need to login for using our services. After Login the user or attacker can upload the clean or infected file on the site. The site allows some limited type of extension at start later on we'll make it suitable for other extension. When a user / peer uploads a file the file gets stored in the database, and is ready for download by other user in P2P system. The user or peer can view or download his own file and the file uploaded by other peers in their proximity. When the other user different from the uploader checks the files available for download he can Scan first before download there's one additional feature of scanning the file. This Algorithm scan the stream of file first and tells it is infected or not. This checking is done on the basis of a key if the file contains a 20-bit long infection key then the file is considered as an infected file. For safety of peer the user cannot download this file on his PC which avoid the attacks of Service based.

4. METRICS

All peers present in the network are equal in computational power and responsibility. There is no Privileged, centralized or trusted peers to manage the information. A peer provide and use services.

Talking about an interaction it is a File Download.

4.1 Preliminary Notations

A peer is denoted p, ith peer is denoted as p_i. Interactions are always unidirectional because when peer p_i downloads a file from peer p_j any of information of interaction is not stored on p_j. If two peer, suppose p_i and p_j had an interaction then the both peer is considered as acquaintance. Every peer stores a record of past interaction known as service history, sh_{ij} denotes service history of p_i with p_i.

After an interaction completed the node downloading the file evaluates quality of service and sets a satisfaction value for the interaction. The importance of an interaction is called weight value, it means the importance of the file according to us. There is one important parameter known as fading effect it means that old interaction must lose its importance as soon as new interaction takes place.
Satisfaction is denoted as 's'
Weight is denoted as 'w'
Fading Effect is denoted as 'f'

4.2 Service Trust Metrics

Finding out the acquaintance's trustworthiness in the service context, two beliefs are calculated, they are "integrity belief" and "competence belief" on the basis of information in its service history. Competence belief states that how well the service provided by a peer in the past it is a kind of aggregate .Integrity belief states that with the help of competence belief we can guess the future trust of a peer.

Let cb_{ij} represents the competence belief of p_i about p_j in the service context. In short competence is an average behavior of past interaction. Evaluation of competence belief the instruction are consider on two parameters, recentness and weight.

Competence Belief:

$$cb_{ij} = \frac{1}{\beta_{ij}} \sum_{k=1}^{sh_{ij}} (s_{ij}^k . w_{ij}^k . f_{ij}^k) \quad (1)$$

Integrity Belief:

$$ib_{ij} = \sqrt{\frac{1}{sh_{ij}} \sum_{k=1}^{sh_{ij}} (s_{ij}^k . w_{ij}^k . f_{ij}^k - cb_{ij})} \quad (2)$$

Fading Effect:

$$f_{ij}^{\mu} = \frac{1}{sh_{ij}} \sum_{k=1}^{sh_{ij}} f_{ij}^{k} = \frac{sh_{ij}+1}{2sh_{ij}} \approx \frac{1}{2} \quad (3)$$

Service Trust Metrics calculation:

$$st_{ij} = cb_{ij} + ib_{ij}/2 \quad (4)$$

$$\mathrm{st_{ij}} = \frac{\mathrm{sh_{ij}}}{\mathrm{sh_{max}}}\left(\mathrm{cb_{ij}} + \mathrm{ib_{ij}}/2\right) + \left(1 - \left(\frac{\mathrm{sh_{ij}}}{\mathrm{sh_{max}}}\right)\right. \mathrm{r_{ij}} \quad (5)$$

4.3 Reputation Metrics

Reputation means we check a peer's whole recent history of communication and the judge what is his status in real world, It is used to measure stranger's trustworthiness. There are two sections, we assumed that p_j is stranger to p_i and p_k is an acquaintance of p_i. If p_i wants to calculate Reputation metric between p_i & p_j, it starts Reputation query to collect Recommendation from its acquaintances.
Substitution of Reputation:

$$er_{ij} = \frac{1}{\beta_{er}} \sum_{p_k \in T_i} \left(rt_{ik} . \Pi_{kj} . r_{kj}\right) \quad (6)$$

Substitution of Competence Belief:

$$ecb_{ij} = \frac{1}{\beta_{ecb}} \sum_{p_k \in T_i} \left(rt_{ik} . sh_{kj} . cb_{kj}\right) \quad (7)$$

Substitution of Integrity Belief:

$$eib_{ij} = \frac{1}{\beta_{ecb}} \sum_{p_k \in T_i} \left(rt_{ik} . sh_{kj} . ib_{kj}\right) \quad (8)$$

Reputation Metrics evaluation:

$$r_{ij} = \frac{[\mu_{sh}]}{sh_{max}} \left(ecb_{ij} - eib_{ij}/2\right) + \left(1 - \frac{[\mu_{sh}]}{sh_{max}}\right) er_{ij} \quad (9)$$

4.4 Recommendation Metrics

The Recommendation means giving suggestions or a brief idea about someone else that you can communicate with. The main pre-requisite of recommendation is the peer must communicate with the other peer for giving its recommendation to someone else. After calculating the Reputation metric between p_i and p_j the recommendation trust values based on accuracy of their recommendations is updated by p_i. The Reputation trust metric explains how p_i updates rt_{ik} according to p_k's recommendation.

The following are the three parameters which are calculated about recommendations are satisfaction, weight and fading effect.

Recommendation satisfaction evaluation:

$$rs_{ik}^{z} = \left(\begin{array}{l} \left(1 - \frac{|r_{kj} - er_{ij}|}{er_{ij}}\right) \\ + \left(1 - \frac{|cb_{kj} - ecb_{ij}|}{ecb_{ij}}\right) \Big/ 3 \\ + \left(1 - \frac{|ib_{kj} - eib_{ij}|}{eib_{ij}}\right) \end{array} \right) \quad (10)$$

Recommendation weight substitution:

$$rw_{ik}^{z} = \frac{[\mu_{sh}]}{sh_{max}} \frac{sh_{kj}}{sh_{max}} + \left(1 - \frac{[\mu_{sh}]}{sh_{max}}\right) \frac{\Pi_{kj}}{\Pi_{max}} \quad (11)$$

Competence and Integrity beliefs in recommendation substitution

$$rcb_{ik} = \frac{1}{\beta_{rcb}} \sum_{z=1}^{rh_{ik}} \left(rs_{ik}^{z} . rw_{ik}^{z} . rf_{ik}^{z}\right) \quad (12)$$

$$rib_{ik} = \sqrt{\frac{1}{rh_{ij}} \sum_{z=1}^{rh_{ik}} \left(rs_{ik}^{z} . rw_{ik}^{\mu} . f_{ik}^{\mu} - rcb_{ik}\right)^{2}} \quad (13)$$

Substitution of Recommendation Trust Metric

$$rt_{ik} = \frac{rh_{ik}}{rh_{max}} \left(rcb_{ij} - rib_{ij}/2\right) + \left(\frac{rh_{max} - rh_{ik}}{rh_{max}}\right) \quad (14)$$

5. SNAPSHOTS

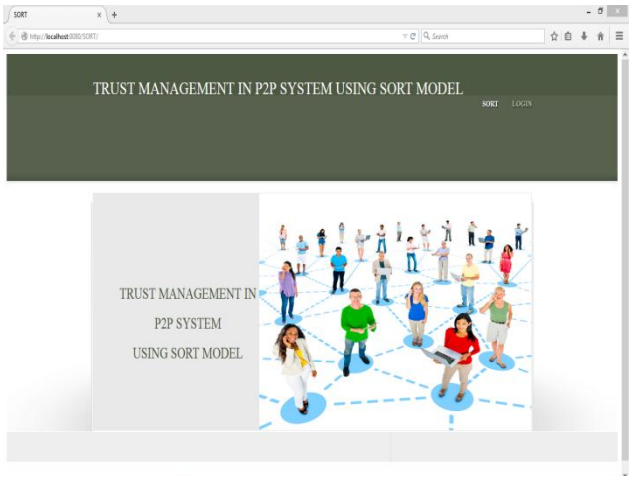

Fig 5.1: Home Screen

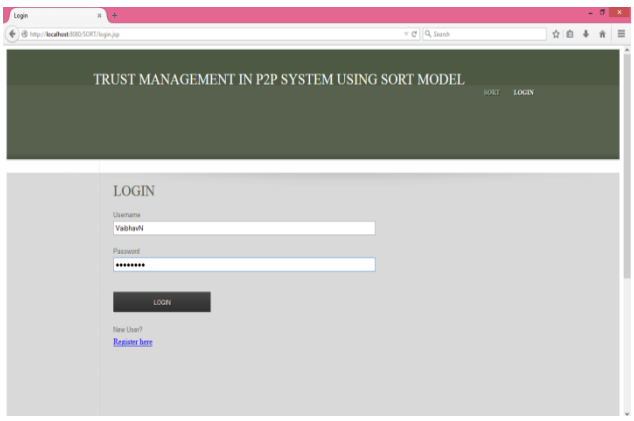

Fig 5.2: LOG IN Page

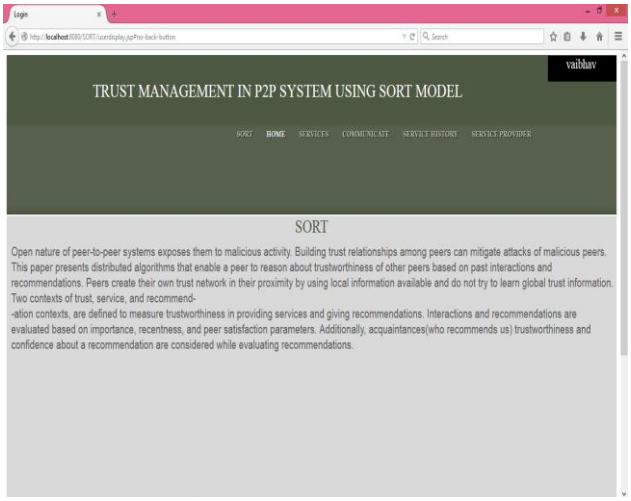

Fig 5.3: USERHOME PAGE

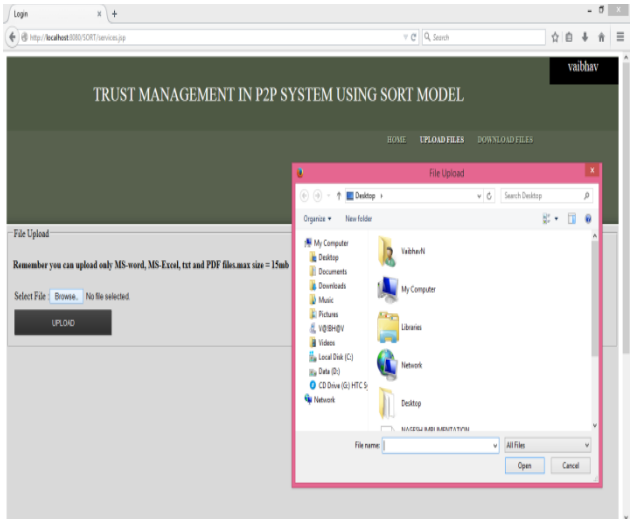

Fig 5.4: File UPLOAD

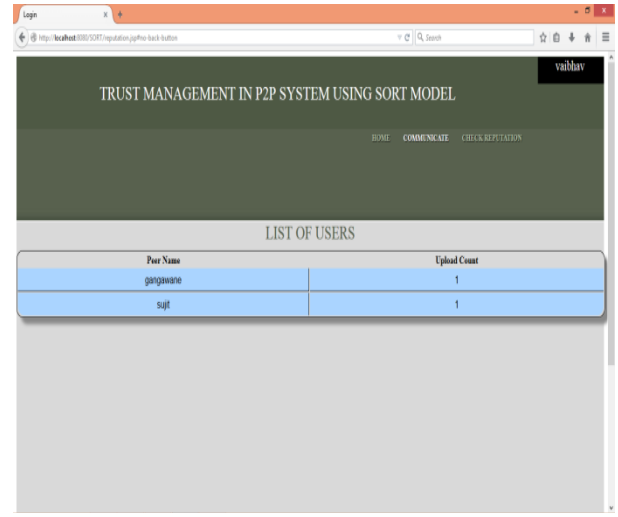

Fig 5.5: LIST of USERS Available:

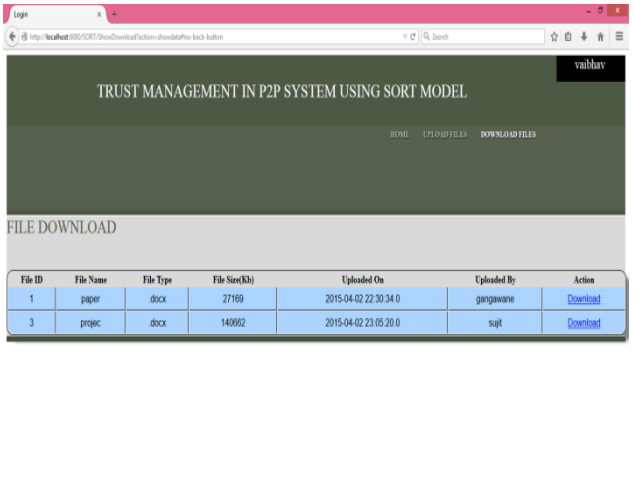

Fig 5.6: FILE Download Page:

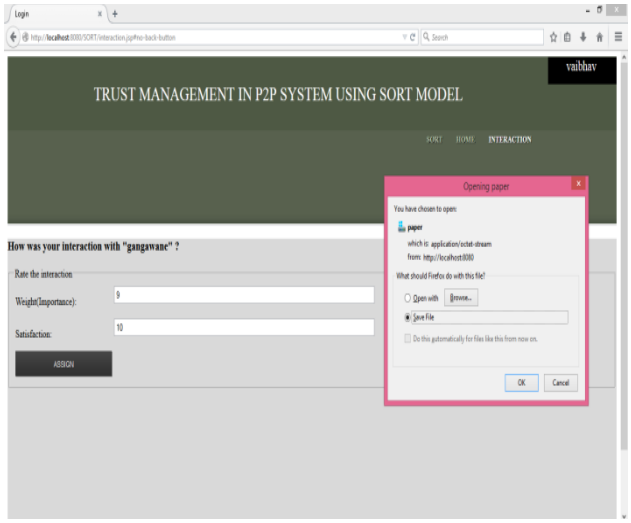

Fig 5.7: After Download set Values of our satisfaction

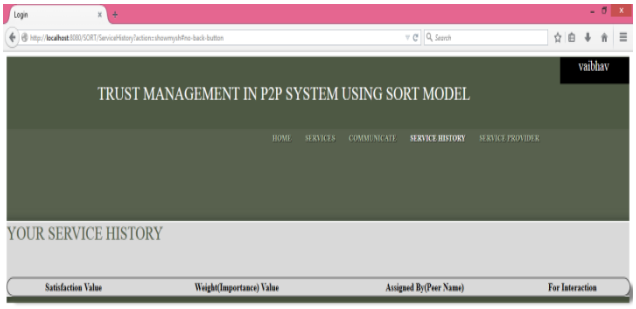

Fig 5.8: SERVICE HISTORY PAGE

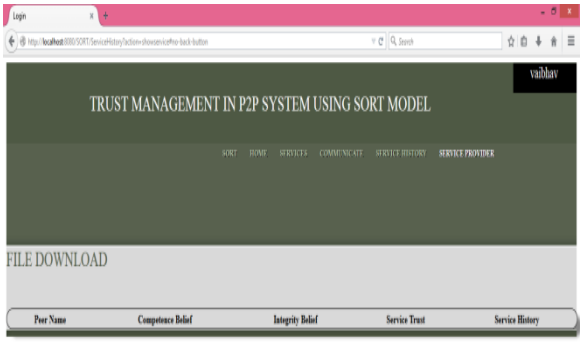

Fig 5.9: SERVICE PROVIDER PAGE

6. CONCLUSION

In this paper we are representing a trust model for P2P networks, in which trust information is created on every user i.e. Peer connected in the network. Taking into consideration of this information the peer can segregate the trusted and malicious peer in its proximity. The two metrics of trust are service and recommendation are used to define capability of providing a service by a peer. An Interaction is unidirectional transferring of a file i.e. download, and recommendation contains the recommender's own experience about the peer with the parameter known as satisfaction, weight and fading effect. Parameters are provided for better assessment of trustworthiness of a peer.
The SORT model helps to mitigate the attacks based on service and recommendation in most of the situations. The main problem in the SORT model is that if a peer changes it identity or access to network the trust information calculated using SORT is affected because the same node is again attached newly to an network and thus making its identity as a stranger to the other peers in the network. Using the credential information about the trust hardly solves all the problem related the security in P2P systems but it is a new way to prohibit the infection done in the network.

ACKNOWLEDGEMENTS

We would like to thank a few people who were closely involved in the completion of this endeavor. Through this acknowledgement, we express our gratitude to all those people who have been associated with this paper and have helped us with it. We thank Dr. Sachin Admane, The Principal of Imperial College of Engineering and Research, Prof. Satish Todmal, The Head of Computer Department, Prof. Darshika Lothe, Lecturer cum Guide who have cooperated with us at different stages during the preparation of the paper.

REFERENCES

[1] *"SORT: A Self ORganizing Trust Model for P2P Systems"* Ahmet BurakCan, Member, IEEE, and Bharat Bhargava, Fellow, IEEE.

[2] *"Trust Management in P2P system using SORT model",* Vaibhav Naik, Vikas Kapre, Amol Gangawane and Sujit Mendhe, all are Final Year in S.P. Pune Univeristy.

[3] K. Aberer and Z. Despotovic, *"Managing Trust in a Peer-2-Peer Information System"* Proc. 10th Int'l Conf. Information and Knowledge Management (CIKM), 2001.

[4] P. Druschel and A. Rowstron. *Past: A large-scale, persistent peer-to-peer storage utility*. In Proceedings of the 18th ACM Symposium on Operating Systems Principles (SOSP'01), October 2001.

[5] J. Heidemann, F. Silva, C. Intanagonwiwat, R. Govindan, D. Estrin, and D. Ganesan. Building efficient wireless sensor networks with low-level naming. In Proceedings of the 18th ACM Symposium on Operating Systems Principles (SOSP'01), October 2001.

[6] Y. Zhong, *"Formalization of Dynamic Trust and Uncertain Evidence for User Authorization,"* PhD thesis, Dept. of Computer Science, Purdue Univ., 2004.

[7] S. Xiao and I. Benbasat, *"The Formation of Trust and Distrust in Recommendation Agents in Repeated Interactions: A Process- Tracing Analysis,"* Proc. Fifth ACM Conf. Electronic Commerce (EC),

BIOGRAPHIES

Vaibhav Naik, Final Year Graduate Student, pursuing his Bachelor of Engineering Degree in Computer Science at "JSPM's Imperial College of Engineering and Research", under "S.P. Pune University", Pune.

Vikas Kapre, Final Year Graduate Student, pursuing his Bachelor of Engineering Degree in Computer Science at "JSPM's Imperial College of Engineering and Research", under "S.P. Pune University", Pune.

Sujit Mendhe, Final Year Graduate Student, pursuing his Bachelor of Engineering Degree in Computer Science at "JSPM's Imperial College of Engineering and Research", under "S.P. Pune University", Pune.

Amol Gangawane, Final Year Graduate Student, pursuing his Bachelor of Engineering Degree in Computer Science at "JSPM's Imperial College of Engineering and Research", under "S.P. Pune University", Pune..