IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 6, June 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

Fogging : Disclosure of Data Breach Attack In Cloud Network.

Saniket M. Kudoo[1], Prof. Dilip Motwani

[1] Department of Computer Engineerig,Vidyalankar Institute Of Technology
Wadala,Mumbai,India (ME Student)

[2] Department of Computer Engineerig,Vidyalankar Institute Of Technology
Wadala,Mumbai,India

Abstract

In Today's generation Cloud Computing or cloud data storage growing as an emerging technology needed for every instances in industry and cloud represent one of the most significant shifts in information technology. Many of us are likely to see in our lifetime.

Cloud computing is becoming the new era for the IT industry, providing development and innovations of networking technology like centralize storage of big data and network services that have the potential to bring data transmission performance, remote data accessibility ,security and privacy and inefficient architecture to the next level.

With these new computing techniques new security challenges arises of the confidential data. Data theft is the biggest challenge faced by cloud service providers or cloud storage. Existing mechanism in industry have failed time to time for many of reasons to maintain data security. The threat of data compromise increases in the cloud, due to the number of and logs between risks and challenges which are either unique to cloud network , or more dangerous because of the architectural or operational characteristics of the cloud environment. Cloud service providers CSP users and various enterprises with various availabilities to store and access their data in third-party data centers.

Cloud's common computing resource is capable of sharing different people at a time from anywhere. We proposed new different technique for securing data in cloud data center with fog networking. We monitored data access in cloud data center environment and logs of user behavior techniques , detects abnormal behavior of user data access patterns.

In search pattern of user or cloud usage abnormal pattern is suspected and then verified using challenge question then we launch disinformation to the user with fog networking to the attacker this will protects against companies real data to be hacked.

Keywords: fogging , cloud computing, fog computing , data theft attack, cloud security

1. Introduction & background

Cloud computing has its own multiple resources , one of them is common that is capability of sharing resources to different people at the same time from different locations. as it allows many organizations to have the opportunity to use Internet-based services SAAS: software as a service, IAAS: infrastructure as a service, PAAS: platform as a service, so that user can save start-up costs, infrastructure capital expenditures, internet use services on a pay-as-you-use basis, access applications only as needed, and quickly reduce or increase capacities of resources.

The existing mechanisms into the cloud field only facilitate security features to data and they are not able to allow for detection of invalid access and thereby its prevention to enable valid distribution of data. The proposed mechanism gives security features to data and thereby allows for detection of invalid access and thereby its prevention to enable valid distribution of data.(1)

In day to day era of cloud computing most of the small and medium scale businesses are increasingly outsourcing for data and computation to the cloud.(3) This obviously supports better operational efficiency with no man power, but comes with greater risks, perhaps the most serious of which are data theft attacks. This is considered as one of the top thread to the cloud computing by cloud security alliance.(CSA)(4)

A data breach is an incident that involves the unauthorized or illegal viewing, access or retrieval of data by an individual, application or service , The data breach attack at Target, resulting in the loss of personal bank information and credit card information of up to 120 million individuals, was one of the series of startling thefts that took place during the normal processing and storage of data.(9) "Cloud computing introduces significant new avenues of attack," said the CSA report authors. The important aspect security of hypervisor operation for cloud environment and virtual machine operations is still to be proved. While data loss and data leakage are both serious issues (1) to cloud computing, the measures you put in place to mitigate one of these threats can compound the other, compression protects data at rest, but lose the encryption key and you've lost the data, so sometimes encryption also fails.

The cloud routinely makes copies of data to prevent its loss due to an unexpected die off of a server. The more copies, the more exposure you have to breaches.(8)
Twitter account incident is one of the famous incident of data theft attack from the cloud. Among the several twitter corporate and personal documents were ex-filtered to tech-crunch which was one of the technological website. The U.S. President Barak Obama's account were illegally accessed. The attacker used administrative password to gain access for various corporate documents hosted on google docs from google infrastructure.
After stealing the customers confidential information or password the attacker get access to all customer data while the user has no means of detecting this unauthorized access.
Deep research and study in cloud computing security domain has demanded for preventing illegal unauthorized access to data by implementing access control protocol and encryption technique. However these techniques have not been able to meet customers data protection. Van dijk and juels have shown that fully homomorphic encryption(3) often acclaimed as solution to such threads is also not sufficient data protection mechanism when used alone. (12).

2 RELATED WORK

From our literature study we identify the following threats to initial document and also suggested and listed by committee of CSA : cloud security alliances "Top Threat To Cloud Computing" are(1)

2.1 Threat 1 : Nefarious use of cloud computing
IaaS cloud providers offer their customers the illusion of unlimited computing network, and storage capacity bundled with frictionless registration process where anyone with a valid credit card can register using cloud services. By abusing the relative anonymity behind these registration and usage models, intruders , malicious code authors, and other hackers have been able to conduct their activities with relative impunity. PASS providers have traditionally suffered from this kind of attack.(1)

2.2 Threat 2 : Insecure interfaces and APIs
Cloud service providers expose a set of software interfaces like application software or APIs that customers use to manage and interact with cloud services. The security of general cloud services is dependent upon the security of these basic APIs. From validation and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to prevent policy. It also increases risk. APIs exposes organizations to a variety of security issues related to confidentiality integrity, availability and accountability.(1)

2.3 Threat 3 : Malicious insiders
This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, For example, a provider may not reveal how it grants employees access to physical and virtual assets, how it keeps track on these employees, or how it analyzes for their data.(12)

2.4 Threat 4 : Shared technology issues
Cloud service providers deliver their services in a scalable way by sharing infrastructure as per user customization like operating system, CPU caches, GPUs, processors etc. which were not designed to offer strong isolation properties for a multi-tenant architecture of given networking. (1)To covered this gap, a virtualization machine monitors mediates access between guest operating systems and the server physical compute resources. Still, even firmware's or hypervisors have built in flaws that have enabled guest operating systems to gain inappropriate levels of control or influence on the customized underlying platform. Strong compartmentalization should be employed to ensure that individual customers do not impact the networking operations of other tenants running on the same cloud service provider. Same service providers Customers should not have access to any other ISP 's actual or residual data, network traffic, data packets etc

2.5 Threat 5 : Data loss or leakage
The threat of data compromise or leakage of data increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment. Various time intruders or untrusted user are the reasons for data loss which can have a devastating impact on a business.(1)

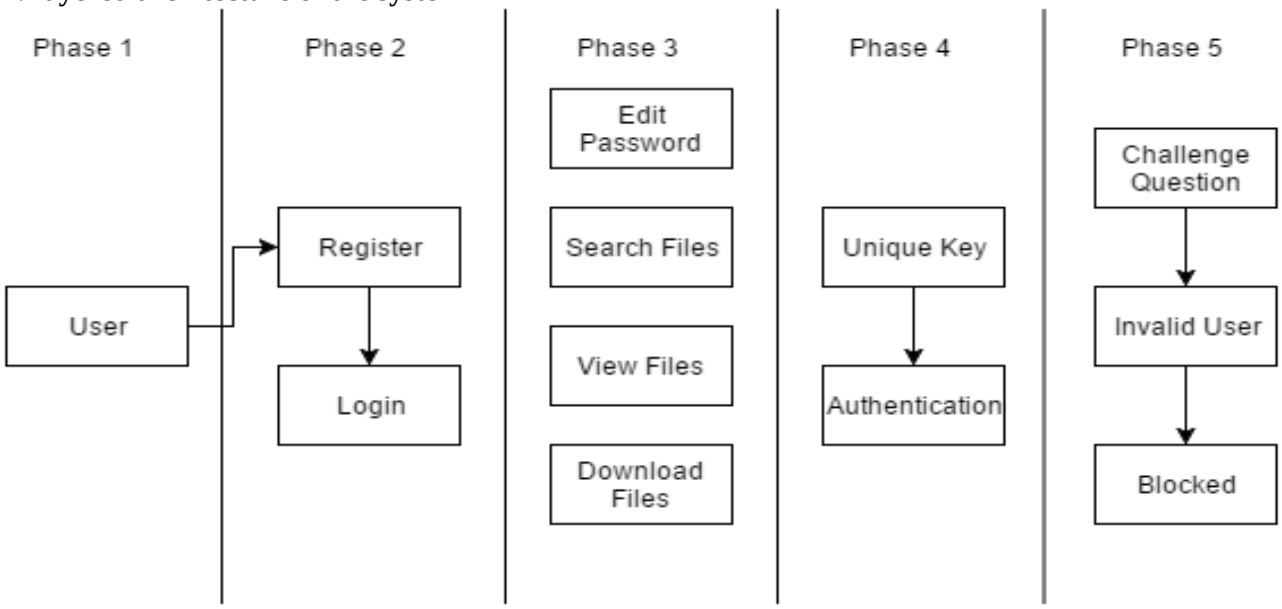
3. Problem statement

Detail research in Cloud computing security has focused on ways of preventing untrusted and illegitimate access to data by maintaining sophisticated access control and encryption mechanisms. However these mechanisms have not been able to prevent data compromise. Building the trust cloud is not enough but also you have to give assured authentication for data protection to the user because accidents of intruders and attacker continues happens and once we lost our confidential data we are not able to get it back.(12)

IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 6, June 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

The basic idea of this paper will recognized or keep monitoring on user behavior or logs into the cloud for daily routine work. Generally daily routine employee has limited search and digital work into the cloud environment. User pattern search technique will continually monitored or keep track on every moment performing into cloud to check weather access is normal access or abnormal access. This method called behavior based profiling technique generally used in theft detection system. Such mechanism would naturally include lot information in cloud environment that to monitor which documents are accessed by whom and how it is accessed often. These simple user specific feature can apply to the system into cloud domain to recognized trusted or untrusted user.

4.Layered architecture of the system



5.1 User Behavior pattern

Generally it is expected that every time access to the user information to any cloud will exhibit normal means of access from a normal user. User profiling pattern technique will work here for the model to analyze how much data user is accessing and what type of data user is accessing in the cloud environment. Such normal user behavior pattern will be continuously checked to determine whether user is normal user or abnormal user. This method of behavior based mechanism is commonly used in fraud detection application or technique.(10)

Behavioral analytics(2) like utilizes user data captured while using the web application, game, or website or any cloud environment is in use by analytic platforms like Google Analytics. Users Platform traffic data like navigation paths, users clicks, users social media interactions is all recorded.(6)

These simple user specific feature can helpful to detect abnormal or untrusted access in cloud based upon the scope and scale of data transfer.

The untrusted user who gets access to the victims systems illegitimately is unlikely to be familiar with the structure and content of the cloud system. Their search is likely to be widespread and untargeted. Based on this key assumptions we profiled user search behavior and developed user models trained with a one class modeling technique.(12)

5.2 Decoy technology for behavior pattern

Decoy documents is like document containing fake information honeyfiles , honeypots and other type of various bogus information generated on demand and provided as a means of captured unauthorized access as a “poison” to thief’s ex-filtered information.(11)

The decoy files are downloaded by the legitimate user and placed in highly accessing locations that are not likely to cause any interference with the normal user activity in the cloud. We placed traps within the file system , the traps are decoy files downloaded from a fog computing site which is an automated service which gives you several types of decoy documents such as bank passbook records , bank password database, bank customers credit card details and medical records etc.

These decoy files were automatically retrieve to the untrusted user once that particular user declared as invalid user. To make decision about to declare particular user as invalid or valid user we monitor their behavior properties of accessing network.

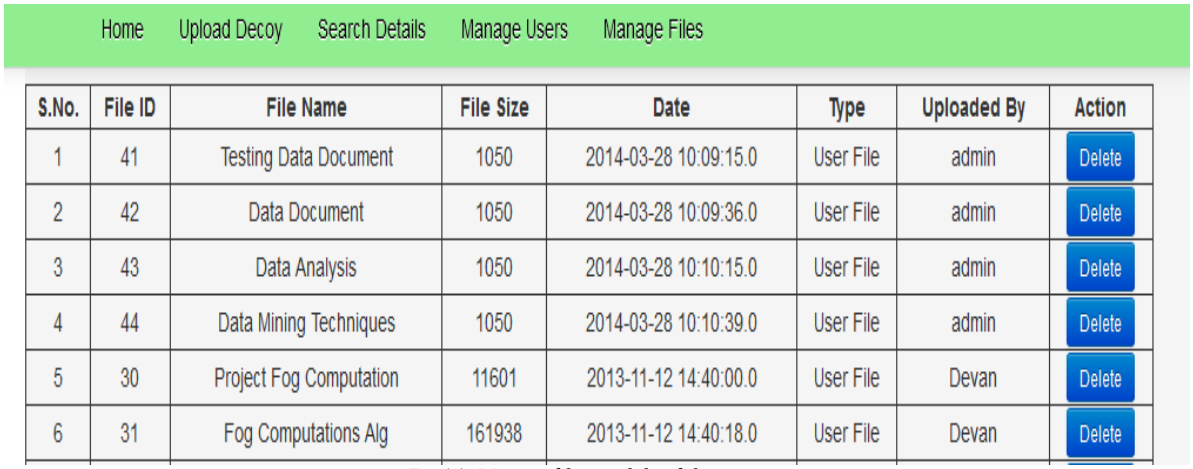
IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 6, June 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

5.3 Fogging : Experimental flow

Generally normal user will register to use cloud space as registering he would suppose to give details of individual profile and company department. As completing the registration process the user will get the taxonomy as per department session and depends on department session user will able to use documents of company or individual.

While registering the new user to the cloud environment user would get the new username and new password suggested by the user itself. Apart from the password which user has chosen the system will generate one random key which would be unique to all the users of the system for future purpose of user. After generation of random key the system will ask for challenge question to every new registering user which is again for future purpose in presence of security of cloud.

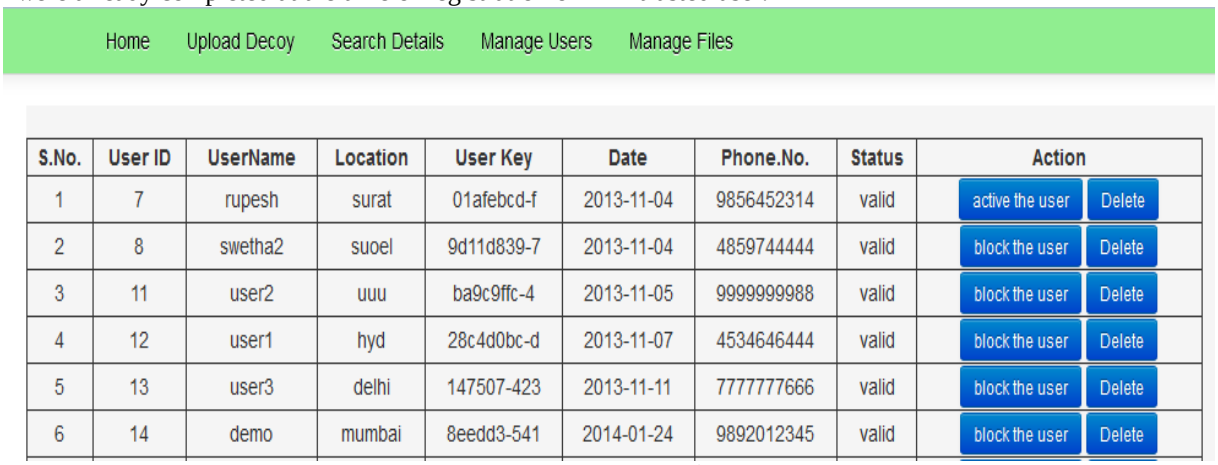
When every user will use the system for accessing the files uploading the files or referring the documents which are available at that time every trusted user have limited search to their files and domain depend on their search pattern every activity would be recorded to secure cloud data. Apart from legitimate user if untrusted user got the access to the cloud then this illegitimate user search techniques will be different as compared to the normal trusted user. If such user is suspected then system will differentiate that user as a invalid user, and get him to the decoy documents which are already uploaded by the system administrative department into the system depend on this illegitimate user will get the decoy stuff which is not worth of any for untrusted user.



S.No.	File ID	File Name	File Size	Date	Type	Uploaded By	Action
1	41	Testing Data Document	1050	2014-03-28 10:09:15.0	User File	admin	Delete
2	42	Data Document	1050	2014-03-28 10:09:36.0	User File	admin	Delete
3	43	Data Analysis	1050	2014-03-28 10:10:15.0	User File	admin	Delete
4	44	Data Mining Techniques	1050	2014-03-28 10:10:39.0	User File	admin	Delete
5	30	Project Fog Computation	11601	2013-11-12 14:40:00.0	User File	Devan	Delete
6	31	Fog Computations Alg	161938	2013-11-12 14:40:18.0	User File	Devan	Delete

Fig (1): Manage files module of the system.

If any normal user pattern got match with the illegitimate user then system will ask him for the challenging question which were already completed at the time of registration of the user. If user would be able to give correct answer of challenge question then this normal user would remain trusted user.



S.No.	User ID	UserName	Location	User Key	Date	Phone.No.	Status	Action
1	7	rupesh	surat	01afebcd-f	2013-11-04	9856452314	valid	active the user Delete
2	8	swetha2	suoel	9d11d839-7	2013-11-04	4859744444	valid	block the user Delete
3	11	user2	uuu	ba9c9ffc-4	2013-11-05	9999999988	valid	block the user Delete
4	12	user1	hyd	28c4d0bc-d	2013-11-07	4534646444	valid	block the user Delete
5	13	user3	delhi	147507-423	2013-11-11	7777777666	valid	block the user Delete
6	14	demo	mumbai	8eedd3-541	2014-01-24	9892012345	valid	block the user Delete

Fig (2): Manage users module of the system

We implement different mechanism to securing the cloud environment using decoy information technology that we have come to call Fog Computing. We used this technology to launch fog information attacks like disinformation attack against malicious intruders , insiders theft preventing them for distinguishing the real sensitive customer data from fake Cloud fog computing data.(12)

6. HMAC unique key

A key hash message authentication code (HMAC) is a specific logic of construction for calculating message authentication code containing cryptographic hash function in combination of secret cryptographic key. (5) As with any message authentication code it may be used to simultaneously verify both the authentication of a message and data integrity. Generally an iterative hash function breaks up a message into blocks of fixed size and iterate over them with a compression function like MD-5 and SHA-1 operates on 512 beats blocks. The size of the output is same as that of the underlying hash function that is 128 or 160 bits in the case of MD-5 or SHA-1 although it can be truncated if desired. (5)

$$HMAC(K,m) = H\Big((K \oplus opad) \;||\; H\big((K \oplus ipad) \;||\; m\big)\Big)$$

Where H is a cryptographic hash function, K is a secret key padded to the right with extra zeroes to the input block size of the hash function and if it is longer than the block size, m is the message to be authenticated. || denotes concatenation , K EXOR outer padding & K EXOR inner padding.(5)

For every user registration system generate a unique key for accessing the cloud environment. We placed some decoy files via admin for disinformation attack to the illegitimate user these decoy files also contain hmac coded information to the untrusted user.

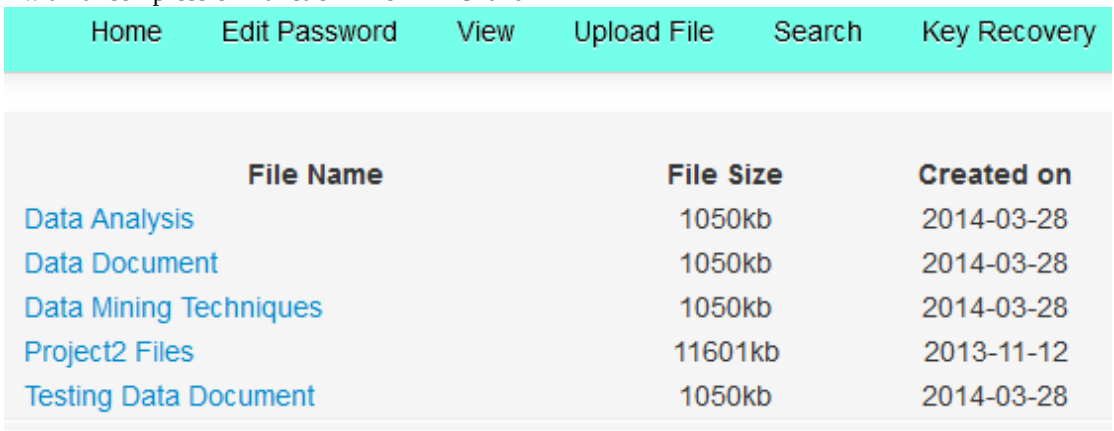


Fig (3) : Cryptographic hash function files

7. Conclusions.

In this paper we have executed novel approach to secured personal and business data in cloud. Encryption or other security mechanisms transactions failed to prevent insider data theft attacks, because of the attacker's has the valid user name and password. Fog Computing is an approach to prevent unauthorized and illegitimate access to the data with sophisticated access controls into the cloud. Hence, proposing an efficient strategy for quickly adopting the user's behavior. The main concept is that to secure the cloud with decoy information technology and is called as "Fog Computing". Confusing the attacker with bogus information that we have concluded and prevented cloud network with the decoy information.

8. Acknowledgement

This material is based on work supported by Defense advanced Research Project Agency (DARPA) under the Anomaly detection at multiple scales (ADAMS) program. As I wish to express my sincere gratitude to PROF. DILIP MOTWANI (Vidyalankar Institute technology , Wadala) for providing me opportunity to do my research work in cloud – fog computing. I also wish to express my sincere thank to all other staff members of Vidyalankar Institute of Technology ,Wadala.

References

(1) Cloud Security Alliance, "Top Threat to Cloud Computing V1.0," March 2010. Available :https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

(2) M. Ben-Salem and S. J. Stolfo, "Combining a baiting and a user search profiling techniques for masquerade detection," in Columbia University Computer Science Department, Technical Report # cucs-018-11, 2011. Available: https://mice.cs.columbia.edu/getTechreport.php?techreportID=1468

(3) Fog Computing: Mitigating Insider Data Theft Attacks.PDF http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6227695

(4) The permanent and official location for the Cloud Security Alliance Top Threats research is: http://www.cloudsecurityalliance.org/topthreats

(5) FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION : The Keyed-Hash Message Authentication Code (HMAC).pdf

(6) International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.1, January 2013 DOI : 10.5121/ijcnc.2013.5112 171 : A USER PROFILE BASED ACCESS CONTROL MODEL

(7) P. Allen, "Obama's Twitter password revealed after french hacker arrested for breaking into U.S. president's account," March 2010. [Online].Available: http://www.dailymail.co.uk/news/article-1260488/Barack-Obamas-Twitter-password-revealed-French-hacker-arrested.html

(8) Protecting cloud through decoy technology : international journal of technology and engineering science (IJTES) volume 1(9) Dec2013

(9) Data breach attack : https://en.wikipedia.org/wiki/Data_breach

(10) International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.1, January 2013 DOI : 10.5121/ijcnc.2013.5112 171 : A USER PROFILE BASED ACCESS CONTROL MODEL AND ARCHITECTURE

(11) Kiran.M, et.al, International Journal of Technology and Engineering Science [IJTES]TM Volume1[9], pp: 1364-1366, December 2013 ISSN: 2320 – 8007 1364 Protecting Cloud through Decoy Technology.

(12) International Journal of Innovative Research in Computer and Communication Engineering *(An ISO 3297: 2007 Certified Organization)* Vol. 4, Issue 1, January 2016 Copyright to IJIRCCE DOI: 10.15680/IJIRCCE.2016. 0401032 168 Fog Computing: Data Theft Detection in Cloud with Behaviour Pattern & Decoy Stuff.

First Author
M.E. Student
Vidyalankar Institute of Technology, Wadala, Mubai University

Second Author
Associate Professor
Department Of Computer Engineering
Vidyalankar Institute Of technology,Wadala,Mumbai.