



AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)

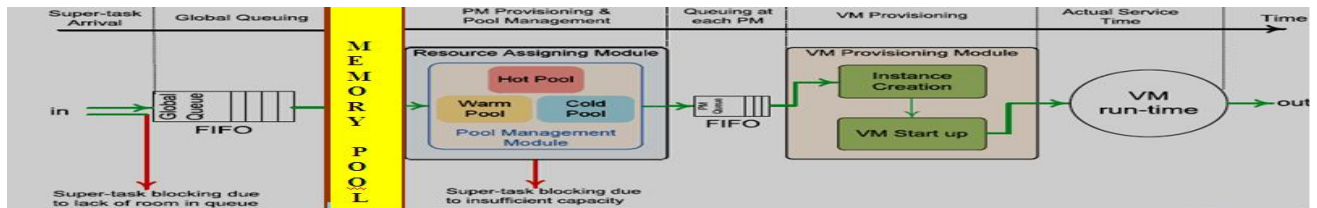


PROJECTS IN DOTNET

IEEE PROJECTS 2013

DN 10001 (JA 6002). GREEN COMPUTING BASED OPTIMIZED RESOURCE UTILIZATION IN CLOUD COMPUTING ENVIRONMENT

ARCHITECTURE DIAGRAM







DESCRIPTION : In the **EXISTING SYSTEM**, Service availability and response time are two important quality measures in cloud's users perspective. In the **PROPOSED SYSTEM**, User's Request is sent to the Global Queue and then to the Resource Assigning Module via FIFO Model. Then we Assign 3 Types of System. First is HOT, in which the Servers will be handling the Jobs Currently, Second is WARM, in which the Servers are kept in Ideal State, then Finally Cold, in which Servers are Turned Off State. Initial Request is send to HOT – Servers, if those Servers are Busy then the Request is forwarded to Warm – Servers, then finally if required to Cold – Servers if both the Hot and Warm Servers are Busy. In the **MODIFICATION** Process, We Develop a Cache Memory Provision, in which Requested Data is Stored in Memory Pool for a Period of Time. If same Data is requested by another user system Verifies the Data is Stored in the Memory pool, then the Data is downloaded from the Memory Pool itself and not by RAM.

ALGORITHM / METHODOLOGY: Successive Substitution Method

DOMAIN: Cloud Computing, Green Computing

IEEE REFERENCE: IEEE TRANSACTIONS on Parallel and Distributed Systems, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10002 (JA 6003). DESIGN AND DEVELOPMENT OF WIRELESS POWER TRANSMISSION FOR CHARGING PHYSICALLY CHALLENGED WHEEL CHAIR AND MOBILE PHONE

ARCHITECTURE DIAGRAM:







DESCRIPTION: In the **EXISTING SYSTEM**, there is no wireless charging is achieved, battery changing of a mobile and wheel chair charging is achieved via manual charging process. It is difficult for physically challenged persons. In the **PROPOSED MODEL**, we are charging a mobile phone through wireless charging system. In the **MODIFICATION PROCESS**, we are implementing Wireless Power Transmission for both wheel chair and mobiles for physically challenged people. Wheel Chair can be controlled by android application and start charging both batteries of wheel chair and Mobile Phones.

ALGORITHM / METHODOLOGY: Wireless Power Transmission

DOMAIN: Mobile Computing, Embedded, Robotics

IEEE REFERENCE: IEEE Paper on Industrial Electronics, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

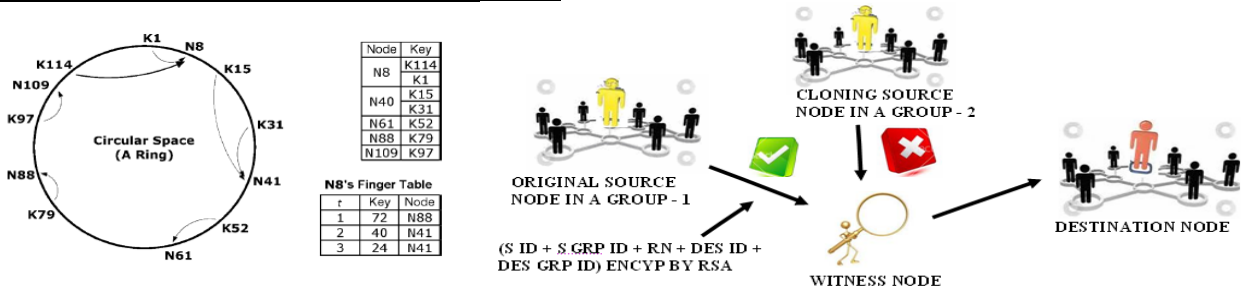
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10003 (JA 6004). IDENTIFICATION OF CLONE NODES USING RDE AND CHORD ALOGORITHM WITH ENCRYPTION

ARCHITECTURE DIAGRAM



DESCRIPTION : In the **EXISTING SYSTEM**, Wireless sensor networks are vulnerable to the node clone, and several distributed protocols have been proposed to detect this attack. So they require too strong assumptions to be practical for large-scale, randomly deployed sensor networks. In the **PROPOSED SYSTEM**, we use two novel node clone detection protocols with different tradeoffs on network conditions and performance. The first one is based on a distributed hash table (DHT) in which Chord algorithm is used to detect the cloned node, every node is assigned with the unique key, before it transmits the data it has to give its key which would be verified by the witness node. If same key is given by another Node then the witness node identifies the cloned Node. The second one is based on the Distributed Detection Protocol which is same as DHT, but it is easy and cheaper implementation. Here every node only needs to know the neighbor-list containing all neighbor IDs and its locations. In the **MODIFICATION** Process, we are implementing RDE protocol, by location based nodes identification, where every region/location will have a group leader. The Group leader will generate a random number with time stamp to the available nodes in that location. Witness nodes verify the random number and time stamp to detect the cloned node. The message is also encrypted for security purpose.

ALGORITHM / METHODOLOGY: CHORD ALGORITHM

DOMAIN: Network Security

IEEE REFERENCE: IEEE Transactions on Networking, 2013

<p>ISO / IEC 20000 CERTIFIED</p>	<p>BHARTIYA UDYOG RATAN - AWARDED</p>	<p>BITS PILANI PRACTICE SCHOOL</p>	<p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------	-------------------------------------------	----------------------------------------	----------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10004 (JA 6011). SECURED DATA STORAGE WITH ENHANCED TPA AUDITING SCHEME USING MERKLE HASH TREE AND MULTI OWNER AUTHENTICATION WITH LOAD BALANCING IN CLOUD COMPUTING

ARCHITECTURE DIAGRAM







DESCRIPTION: In the **EXISTING SYSTEM**, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity. In the **PROPOSED SYSTEM**, a secure cloud storage system supporting privacy-preserving public auditing. In which the Data owner uploads the data in the Cloud Server and they are allowed to modify the data using the Private Key. The Cloud Server Stores the data and split those data into the batches using Merkle Hash Tree Algorithm. The TPA will audit the data files that are requested by the Data Owner. The TPA will also audit the multiple files also. In the **MODIFICATION** process, TPA will also audit the files randomly also; even the files which are not requested by the data owner. We also Provide Load Balancing Technique for speedy data Delivery. Data is securely handled and verified by multi Owner Authentication.

ALGORITHM / METHODOLOGY: Merkle Hash Tree, Load Balancing

DOMAIN: Cloud Computing, Security

IEEE REFERENCE: IEEE TRANSACTIONS on Computers, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

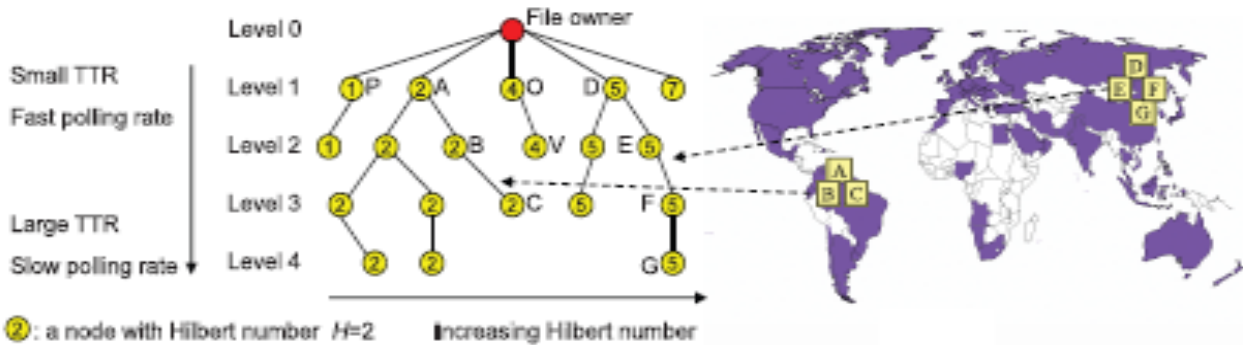
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10005 (NJA 1). DESIGN OF GEOGRAPHICAL REPLICA NODES DISTRIBUTION BASED ON TTR, CHORD, INDEXING TECHN.

ARCHITECTURE DIAGRAM



DESCRIPTION: In the **EXISTING SYSTEM**, File consistency maintenance in P2P systems does not guarantee the updation or modification among the Replica Nodes. It is high overhead.. In the **PROPOSED SYSTEM**, to handle these challenges, this paper introduces a poll-based distributed file consistency maintenance method called geographically aware wave (GeWave). Owner node identifies its Members with respect to its TTR (Time to Refresh) value. The distribution ensures continuous data update among all the replica nodes. We use Chord Algorithm to communicate with Predecessor and Successor Nodes. In the **MODIFICATION**, Index Filter is achieved, Every Root node will maintain the Index data of rest of the Files present in its nearest Root Node. This process helps to search any data very easily.

ALGORITHM / METHODOLOGY: Linear Increase Multiplicative Decrease, Index, Chord

DOMAIN: Networking

IEEE REFERENCE: IEEE Transactions on Parallel and Distributed Systems, 2013



ISO / IEC 20000 CERTIFIED



BHARTIYA UDYOG
RATAN - AWARDED



BITS PILANI
PRACTICE SCHOOL



ISO 9001 : 2008 CERTIFIED



AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10006 (JA 6012). DESIGN AND IMPLEMENTATION OF DATA SANITAZATION TECHNIQUE FOR EFFECTIVE FILTERING WITH ENCHANCED MEDICAL SUPPORT SYSTEM IN CLOUD

ARCHITECTURE DIAGRAM







DESCRIPTION: In the **EXISTING SYSTEM**, thousands of textual documents are publicly published every day. Even though methods to assist the sanitization process have been proposed, most of them are focused on the detection of specific types of sensitive entities for concrete domains, lacking generality and requiring user supervision. In the **PROPOSED SYSTEM**, We are developing this Project for Medical Purpose. Here we use the Cloud Server as a main Server, where all the Data from the Users are Stored. We design this system using Registered Doctors, Paid and unpaid users. Data Sanitization is achieved by Three Process. 1. Entity Generalization-Preserving the Privacy data with its semantics. 2. Entity Swapping is used to Reduce the Document Size. 3. Noise Addition: an entity substituted by another similar one extracted from another repository. In the **MODIFICATION** Process, Paid users are only allowed to access the Doctor’s Opinion/Suggestion/ Prescriptions. Registered Doctors can only Reply to the User’s/ Patients.

ALGORITHM / METHODOLOGY: Data Sanitization

DOMAIN: Data Mining, Security

IEEE REFERENCE: IEEE Transactions on Information Forensics and security, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10007 (JA 6014). DESIGN OF USER'S BEHAVIOR, PATTERN RECOGNITION AND OTP GENERATION FOR ATM THEFT PROTECTION

ARCHITECTURE DIAGRAM



DESCRIPTION: In the **EXISTING SYSTEM**, there is no security layer is implemented in the ATM card expect PIN number. It is very costly for the bank to include the fingerprint and Iris Scanner. In the **PROPOSED MODEL**, we monitor the location of the ATM Usage, time taken for the user to accessing the ATM machine, sequence of events processed by the User and expected amount of withdrawal by the user. All these four factors are verified for the authentication purpose of the user along with password. If any of the above said, parameters are differing, and then the One Time Password is generated to the User's Mobile Number for further more secure authentication system. In the **MODIFICATION PHASE**, an automation User Interest Recognition Model is designed to enhance the User comfortness and detection of time span spend by the User in the ATM machine.

ALGORITHM / METHODOLOGY: Secure Random Number Generation
Algorithm

DOMAIN: Mobile Computing, Security, Embedded.

IEEE REFERENCE: IEEE Paper on Information and Communication Technologies, 2013

 ISO / IEC 20000 CERTIFIED	 BHARTIYA UDYOG RATAN - AWARDED	 BITS PILANI PRACTICE SCHOOL	 ISO 9001 : 2008 CERTIFIED
--------------------------------------	-------------------------------------------	----------------------------------------	--------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

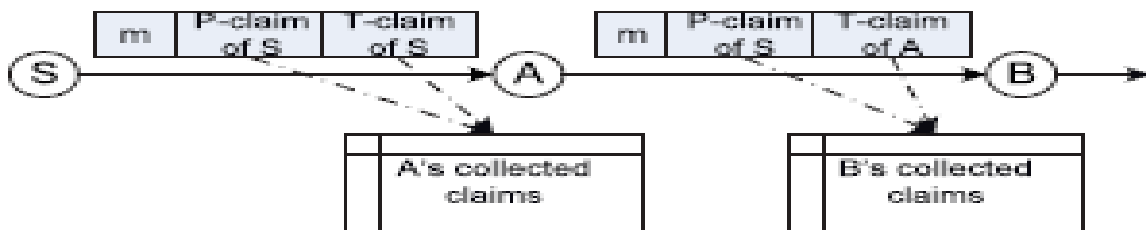
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10008 (JA 6015). DETECTION OF FLOODING ATTACKS AND CONTENT ANALYSIS IN DTN

ARCHITECTURE DIAGRAM







DESCRIPTION : In the **EXISTING SYSTEM**, DTNs consist of mobile nodes carried by human beings vehicles etc. when a node receives some packets, it stores in its Buffer and Forwards to another it contacts another. DTNs are vulnerable to flood attacks which would waste Buffer Resources of DTN. In the **PROPOSED SYSTEM**, each node has a limit over the number of packets that it, as a source node, can send to the network in each time interval (**P-Claim**). Each node also has a limit over the number of replicas that it can generate for each packet (**T-Claim**) (i.e., the number of nodes that it can forward each packet to). The two limits are used to mitigate packet flood and replica flood attacks, respectively. **MODIFICATION** that we propose is to verify the Content of the Data which is transmitted. Sometimes Attackers would transmit a Worm File within P-Claim & T-Claim.

ALGORITHM / METHODOLOGY: Packet Forwarding Scheme

DOMAIN: Network Security

IEEE REFERENCE: IEEE Transactions on Dependable and Secure Computing, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

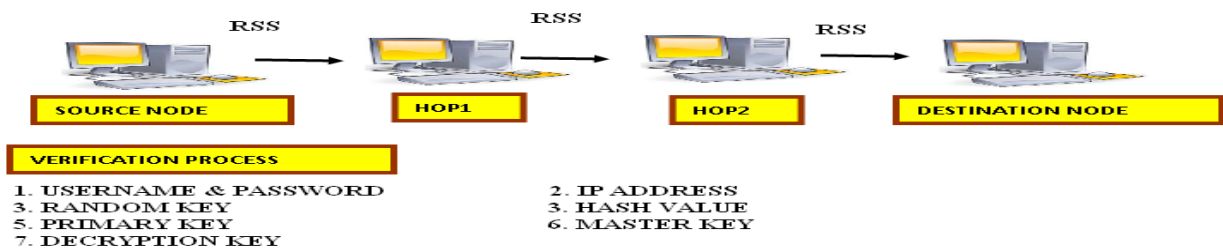
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10009 (JA 6008). SECURED KEY EXCHANGE BASED AUTHENTICATION WITH ENCRYPTION AND HASHING TECHNIQUE USING RECEIVED SIGNAL STRENGTH

ARCHITECTURE DIAGRAM







DESCRIPTION: In the **EXISTING SYSTEM**, Currently, the most common method for establishing a secret key is by using public key cryptography. However, public key cryptography consumes significant amount of computing resources and power which might not be available in certain scenarios. In the **PROPOSED SYSTEM**, Source Sends a Data to the Destination, Data is forwarded to the intermediate Nodes one by one, based on Received Signal Strength (RSS) Secret Key is Generated which is passed to both the Source and the Destination. A Random Key is parsed by both Source and Destination which is exchanged between both for Verification. Both of them Generates Hash Key of the Secret Keys, which is also Verified by both of them only then the Data can be viewed by the Destination. **MODIFICATION** that we propose, is to have a strong Verification Scheme in the Destination End. Destination's User Name, Password, IP Address, Primary Key, Parsed Random Key, Hash Value of Secret Key, Decryption Key to open the Data, as well as Secondary Key for changing the Primary key is verified for the Secured Communication of Data between Source and any Destination.

ALGORITHM / METHODOLOGY: Key Extraction Algorithm

DOMAIN: Mobile Computing, Security

IEEE REFERENCE: IEEE Transactions on Mobile Computing, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

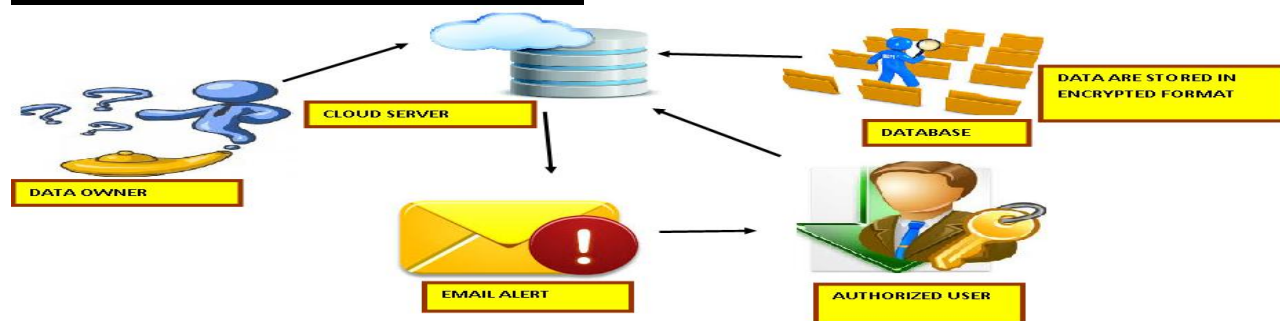
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10010 (JA 6036). IMPLEMENTATION OF ATTRIBUTE BASED ENCRYPTION FOR EFFECTIVE MEDICAL ANALYSIS IN CLOUD COMPUTING ENVIRONMENT

ARCHITECTURE DIAGRAM

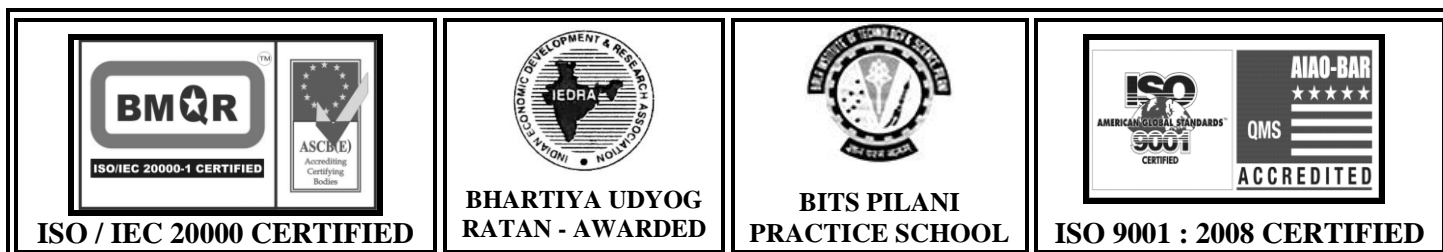


DESCRIPTION: In the **EXISTING SYSTEM**, Personal health record (PHR) is an emerging patient-centric in Cloud Computing Servers. However, there is no Security in keeping privacy concerns of the Patient & could be exposed to those third party servers and to unauthorized parties. In the **PROPOSED MODEL**, a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. We leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios.

ALGORITHM / METHODOLOGY: Attribute based encryption (ABE)

DOMAIN: Cloud Computing, Security

IEEE REFERENCE: IEEE Transactions on Parallel and Distributed Systems, 2013





AADHITYAA INFOMEDIA SOLUTIONS

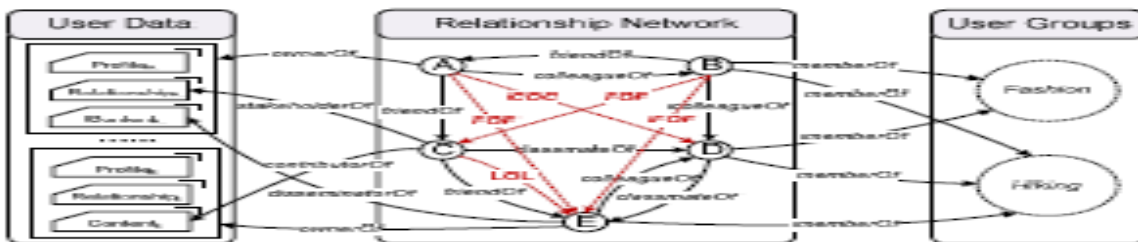
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10011 (JA 6005). DESIGN OF MULTI PARTY ACCESS CONTROL SYSTEM IN SOCIAL NETWORKING ENVIRONMENT

ARCHITECTURE DIAGRAM:







DESCRIPTION: In the **EXISTING SYSTEM**, Online Social Networking Sites like Facebook and Twitter will only allow the Single User to Control the data from accessing. In the **PROPOSED SYSTEM**, we implement Multi Party Access Control Mechanism by which the Users are allowed to share data based on the following Criteria with the relationships between the Users: 1. Data Sensitivity based on the Sensitivity of the data it will shared/ access among the Users. Decision Mechanisms are used to make the decision based on the decision taken by the Multiple Users, and Threshold Mechanisms are used to set the Threshold Values and based on the Threshold values the data will shared. Also we implement can Share the data based on the Majority Permit mechanism in the Majority of the User grant the Permission to access the data. In the **MODIFICATION** Part of this Project is, User can add a person as his / her Friend, Family or General Category. User can post any data and can specify it is Sensitive and Data Sharing to a Particular Category. If unshared Person wants to see the Unshared Data then he / She has to get Permission from the Data Owner, only then the Data is shared.

ALGORITHM / METHODOLOGY: Multiparty Access Control

DOMAIN: Data Mining

IEEE REFERENCE: IEEE Transactions on Knowledge and Data Engineering, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

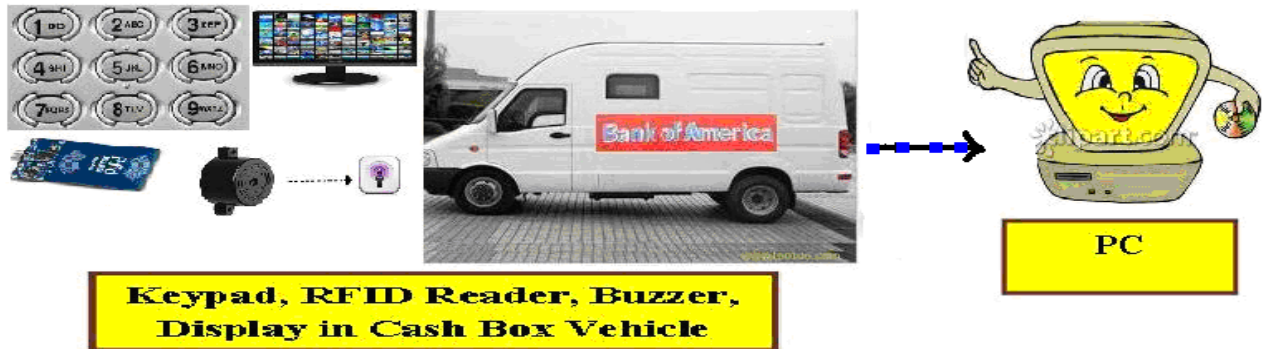
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10012 (NJA 5) . CASH BOX : SECURED RFID BASED LOCATION AND OTP VERIFICATION SCHEME FOR MONEY TRANSPORT VEHICLE

ARCHITECTURE DIAGRAM







DESCRIPTION: In the **EXISTING SYSTEM**, there is no automatic Security system is implemented. We have manual Police Force to protect the Vehicle. In the **PROPOSED SYSTEM**, RFID based security and control system for money transaction vehicles. In real-time GPS will be used to locate the Location tracking, but for ease of implementation we are using RFID based location detection. Each ATM Centers will be provided with a RFID Tag .In the **MODIFICATION** phase, Vehicle is stopped at a particular Location, which is verified by the Server through RFID Card. The server will compare the tag value with the database and if it matches then it will send an OTP number to both money vehicle and to the driver's mobile number as an SMS. Upon receiving the SMS he has type the OTP to let the money box door open.

ALGORITHM / METHODOLOGY: RFID, Random Number Generation

DOMAIN: Mobile Computing, Embedded

IEEE REFERENCE: IEEE Paper on Intelligent Systems, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10013 (JA 6025). MULTI KEYWORD RANKED SEARCH OVER ENCRYPTED CLOUD.

ARCHITECTURE DIAGRAM

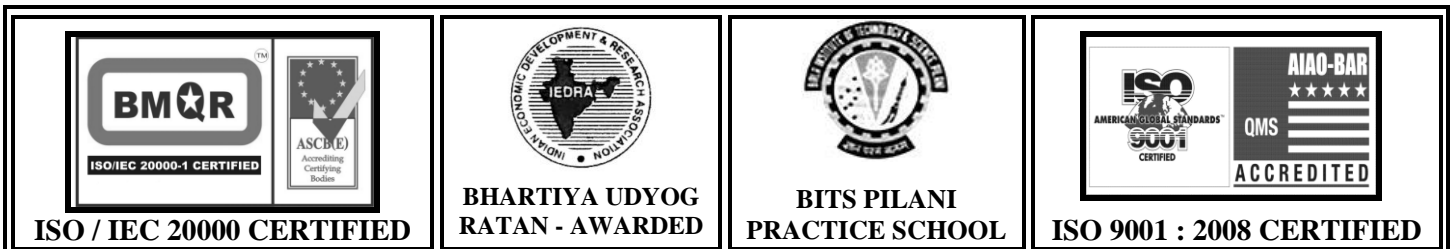


DESCRIPTION: In the **EXISTING SYSTEM**, with the advent of Cloud Computing, Data Owners are motivated to outsource their complex Data Management Systems from local sites to the Commercial Public Cloud for great flexibility and Economic Savings. But data security and privacy is the Major Threat in Cloud Computing. In the **PROPOSED MODEL** the Entire Data Stored in the Cloud Server is encrypted and User's Query is also encrypted. Encrypted Query is sent to the Cloud Server and the encrypted Resultant Data is sent to the User. The **MODIFICATION** that we propose is effective Ranking of the Relevant Data to the user. We use Stemming Algorithm, Ranking Algorithm to find Term Frequency and only the Best Resultant Data is sent to the user using TOP-K-Query Algorithm in the Encrypted Format using RSA Algorithm.

ALGORITHM / METHODOLOGY: RSA Algorithm

DOMAIN: Cloud Computing, Security

IEEE REFERENCE: IEEE Transactions on Parallel and Distributed Systems, 2013





AADHITYAA INFOMEDIA SOLUTIONS

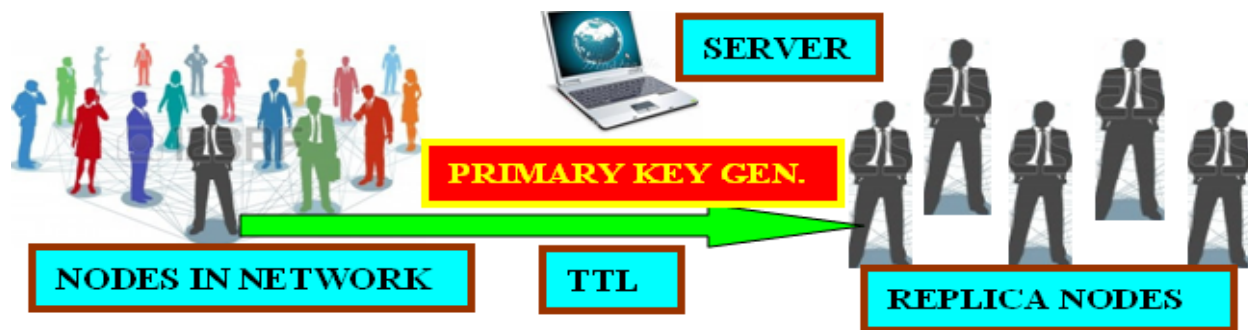
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10014 (NJA 2). DETECTION OF REPLICATION ATTACKS WITH ALTERED PRIMARY KEY USING LOCALIZATION APPROACH & PRIORITY STATUS OF DELIVERY

ARCHITECTURE DIAGRAM







DESCRIPTION: In the **EXISTING SYSTEM**, Defending against Node Replication is not achieved in the Present System, only few methods are deployed. In the **PROPOSED SYSTEM**, using Localization Algorithm to identify the exact place of the original node which is verified and compared with the requested node to detect whether it is Replica or original node. We are monitoring Primary Key for every Node. In the **MODIFICATION**, this Primary Key will be changed on Random basis with Time Stamp & as attack occurs. Source node will specify Time to Live (TTL) for every data Transmission, based on the TTL value Priority of the Packet is identified and transmitted accordingly.

ALGORITHM / METHODOLOGY: Localization, TTL, Key Gen Algorithm

DOMAIN: Network Security

IEEE REFERENCE: IEEE Transactions on Information Forensics and Security, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

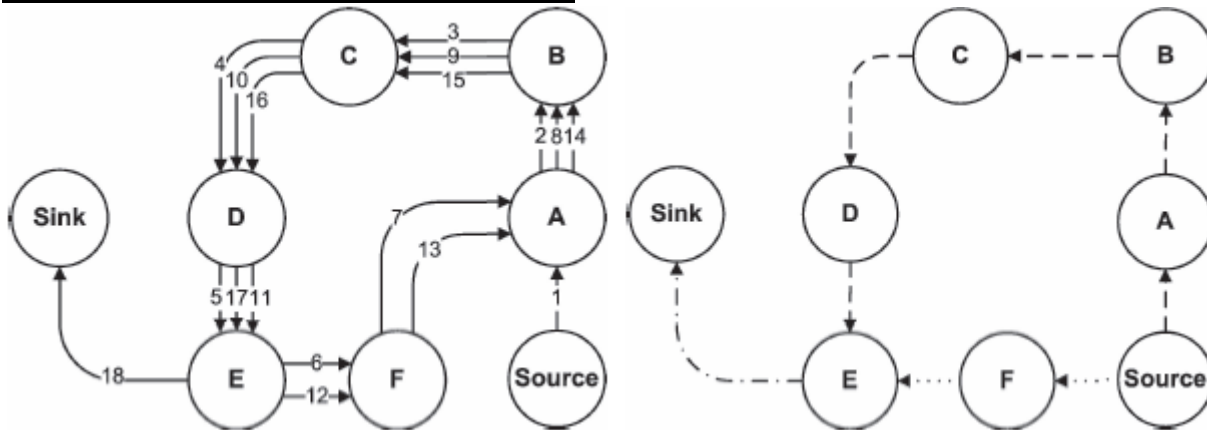
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10015 (NJA 5). DETECTION OF VAMPIRE ATTACKS AND ACTUAL ENERGY LEVEL MONITORING

ARCHITECTURE DIAGRAM



DESCRIPTION: In the **EXISTING SYSTEM**, Vampire attack as the composition and transmission of a message that causes more energy to be consumed by the network than if an honest node transmitted a message of identical size to the same destination. There is no Preventive Mechanism for the detection of Vampire Attacks. In the Proposed System, Vampire attacks will consume lot of Energy by attacking any node in the Network. It also sends the same packets repeatedly via the same node. Our system identifies the sudden Energy lose and the Packets ID to detect this attack. In the **MODIFICATION Part**, We are finding the actual Energy level of all the nodes from the Predecessors and Successors nodes using Chord Algorithm. Attacker node would specify some false Energy level for the attacked nodes. Our Methodology

ALGORITHM / METHODOLOGY: Optimize Discovery, Chord

DOMAIN: Mobile Computing, Security

IEEE REFERENCE: IEEE Transactions on Mobile Computing, 2013

<p>ISO / IEC 20000 CERTIFIED</p>	<p>BHARTIYA UDYOG RATAN - AWARDED</p>	<p>BITS PILANI PRACTICE SCHOOL</p>	<p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------	-------------------------------------------	----------------------------------------	----------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

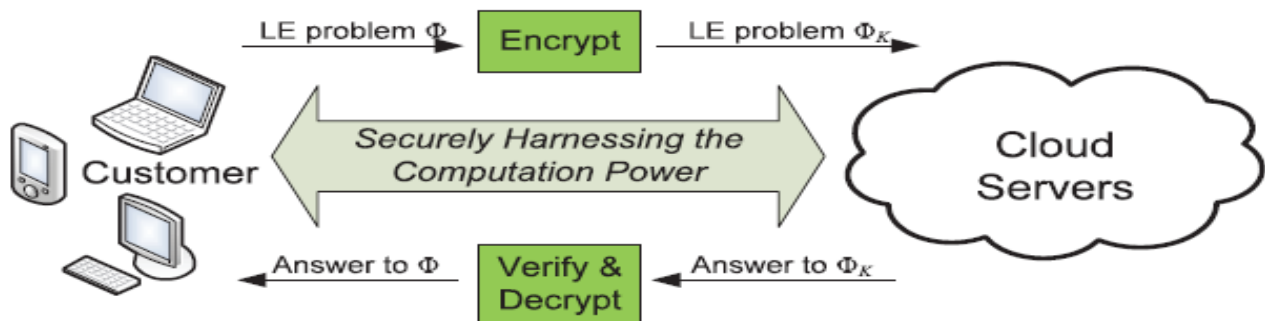
(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3 COMPLIANCE & ISO 9001 : 2008 CERTIFIED SOFTWARE DEVELOPMENT COMPANY)

TRUST ME - CRISIL CERTIFIED



DN 10016 (NJA 8). HARNESSING THE CLOUD FOR SECURELY OUTSOURCING LARGE-SCALE SYSTEMS OF LINEAR EQUATIONS

ARCHITECTURE DIAGRAM







Description: In the **EXISTING SYSTEM**, despite the tremendous benefits, the fact that customers and cloud are not necessarily in the same trusted domain brings many security concerns and challenges toward this promising computation outsourcing model. In the **PROPOSED SYSTEM**, we ensure the security for the data management. Data owner will transmit the data which is encrypted and stored. Primary key is changed with respect to Time stamp. Keys are updated to the data Owner through e mail. After the verification of the Updated Key data owner retrieves the Data. In the **MODIFICATION**, Data Owner will authenticate few registered users for accessing that Data. Same updated Key is sent to registered User's E mail also, So that they can also access the data when ever they require.

ALGORITHM / METHODOLOGY: Iterative Algorithm

DOMAIN: Cloud Computing, Security

IEEE REFERENCE: IEEE TRANSACTIONS on Parallel and Distributed Systems, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

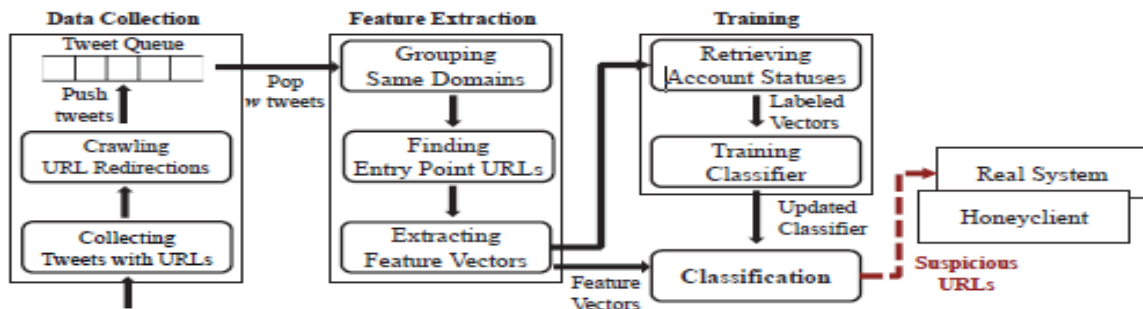
TRUST ME -
CRISIL
CERTIFIED

**(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)**



**DN 10017 (JA 6017). DETECTION AND REMOVAL OF
SUSPICIOUS URLS-PHISING SITE ISOLATION**

ARCHITECTURE DIAGRAM

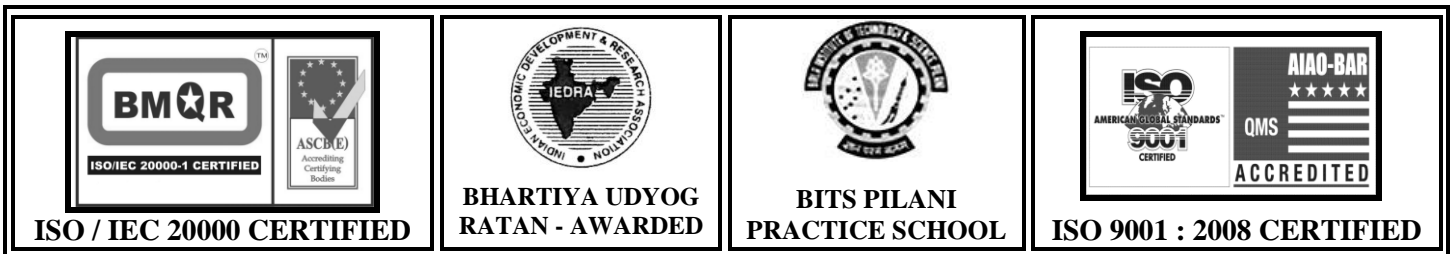


DESCRIPTION: In the **EXISTING SYSTEM**, Twitter is prone to malicious tweets containing URLs for spam, phishing, and malware distribution. Conventional Twitter spam detection schemes utilize account features such as the ratio of tweets containing URLs and the account creation date, or relation features in the Twitter graph. These detection schemes are ineffective against feature fabrications or consume much time and resources. In the **PROPOSED SYSTEM**, we introduce WARNINGBIRD, a suspicious URL detection system, in which we are analyzing the Entry Point URL, URL Length, Origin of the URL, Number of Different landing URLs, Different Domains and IP address, Tweet Text and etc to find the suspicious URL Twitter stream. In the **MODIFICATION** process, we also analyze the web page content which contains the malicious scripts (HTML Content, JavaScript's).

ALGORITHM / METHODOLOGY: Support Vector Classification

DOMAIN: Web Security

IEEE REFERENCE: IEEE Transactions on Dependable and Secure Computing, 2013





AADHITYAA INFOMEDIA SOLUTIONS

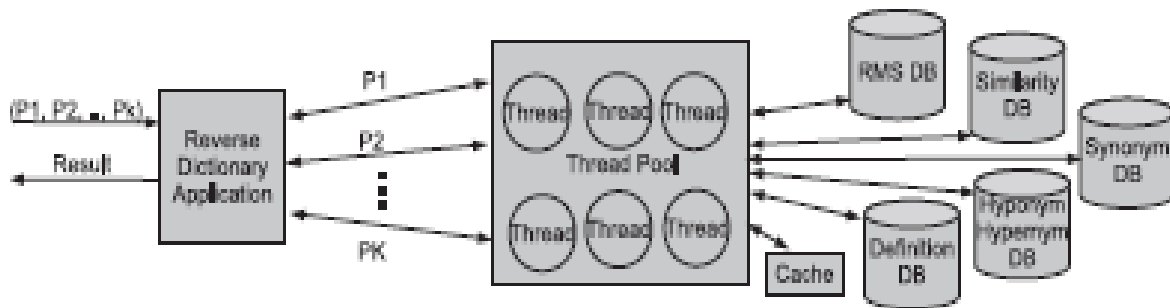
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10018 (JA 6019). BUILDING SCALABLE DATABASE DRIVE REVERSE DICTIONARY

ARCHITECTURE DIAGRAM




DESCRIPTION: In the **EXISTING SYSTEM**, we have implemented only the forward mechanism to search for the Keyword in the dictionary. In the **PROPOSED SYSTEM** we are implementing a Reverse Dictionary by which we can retrieve the data for the User entered Keyword from the database by assigning each Thread to retrieve the result from the Database. Each thread will be assigned for each storage location, so that we can retrieve the exact matched results from that database. In the **MODIFICATION PROCESS**, we also retrieve the exact results for the User entered Phrases which similar to the Entered Keyword. Also we implement Forward dictionary technique to retrieve the data based on the Entered Keyword.

ALGORITHM / METHODOLOGY: Stemming Algorithm

DOMAIN: DATA MINING

IEEE REFERENCE: IEEE Transactions on Knowledge and Data Engineering, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

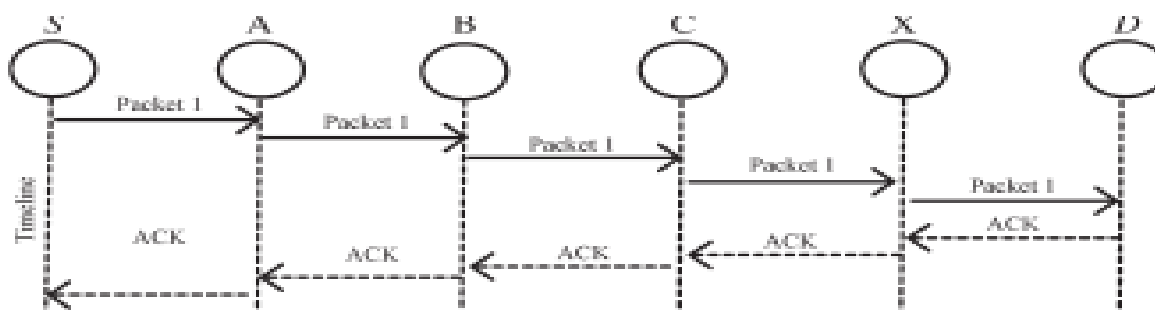
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10019 (JA 6020). IDENTIFICATION OF MISBEHAVIOUR AND PACKET LOSS ACTIVITIES IN MOBILE ADHOC NETWORKS.

ARCHITECTURE DIAGRAM




DESCRIPTION: In the **EXISTING SYSTEM**, due to the lack of security in the MANETs, Because of the Open medium and distribution of the nodes in various locations, makes MANET vulnerable to malicious to attackers. In the **PROPOSED SYSTEM**, The data is send to the Destination Node via intermediate nodes in the Encrypted format. Each node has to pass the Acknowledgement after the Receiving of the data. If any of the nodes didn't pass the Acknowledgement, then the Source Node will send the data to the Destination via another Route. Then the MRA is filed. If the Destination claims Duplication of the Data then Source will find the Misbehavior. If there is no Data, then resend the Data is stored in the Destination, again the packet dropped node is considered as attacker, and then the node is removed from the network. In the **MODIFICATION** Process, the server will identify the buffer level of the intermediate nodes; If the packets are dropped due to inadequate of Space/Memory then the node is not considered as an attacker.

ALGORITHM / METHODOLOGY: Digital signature verification

DOMAIN: Mobile Computing

IEEE REFERENCE: IEEE Transactions on Industrial Electronics, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

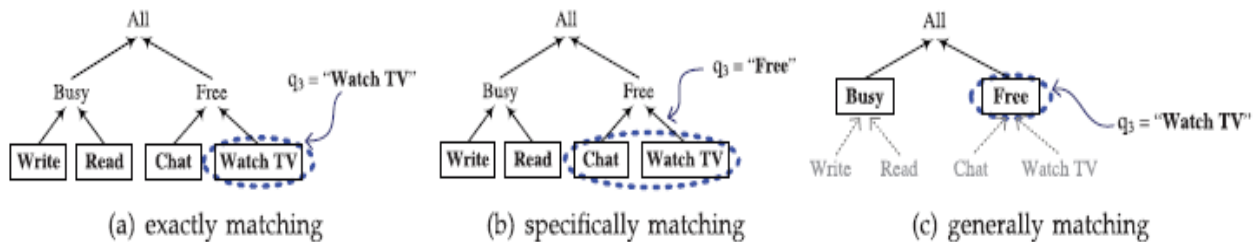
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10020 (NJA 10). CONTEXT BASED SEARCH KEY INFORMATION REFINER

ARCHITECTURE DIAGRAM







DESCRIPTION: In this **EXISTING SYSTEM** the user collecting different type of data from the global web for both read and writing purpose. Also we use lot of key word search the information but they could not remember the key where original queries were wrongly remembered due to their vague or lost memories. In the **PROPOSED SYSTEM** we projected solution for remember the key words to get the information exactly even a month or a year ago. We develop a context-based information refining approach. A system called ReFinder has been implemented to assist users refining Web pages or files based on their previous accessed context including time, place, and concurrent activity In the **MODIFICATION PROCESS**, we projected on not only find the refined queries but also the best web page link visited by the user for that key word or queries. Also we also implement feedback system to the best link found by user for their queries.

ALGORITHM / METHODOLOGY: Cluster-Association-Based Refinding Algorithm

DOMAIN: Data Mining

IEEE REFERENCE: IEEE Transactions on Knowledge and Data Engineering, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

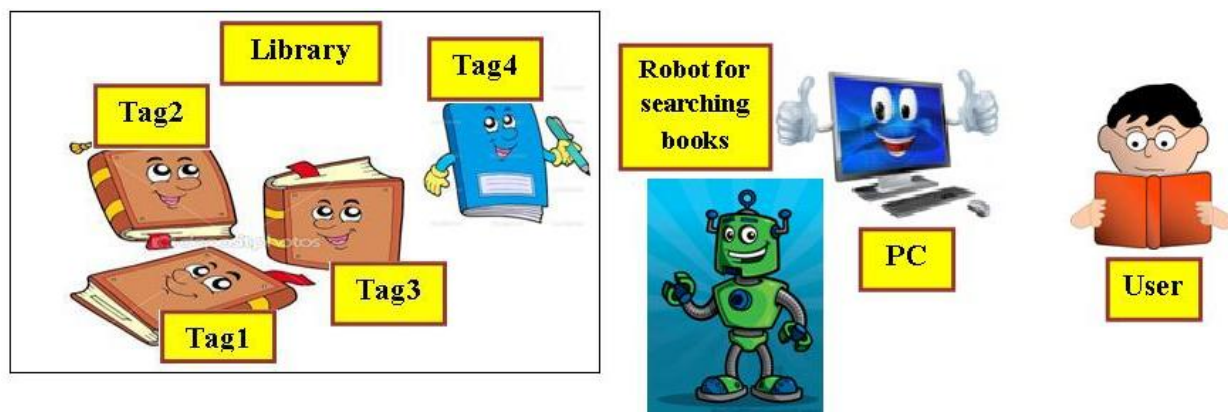
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10021 (NJA 13). AUTOMATIC ROBOT BASED BEST BOOKS IDENTIFICATION AND ANALYSIS OVER LIBRARY USING STEMMING AND RANKING ALGORITHM

ARCHITECTURE DIAGRAM

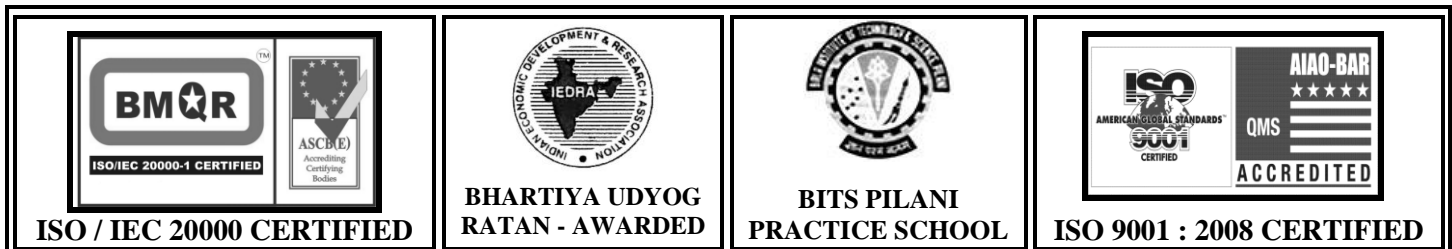


DESCRIPTION : In many **EXISTING SYSTEMS**, only manual process identification of relevant data is maintained. Even in library we search the books in a manual way only. In the **PROPOSED SYSTEM**, the user provides speech input to the Robot via wireless connection with the PC, so that the Robot directs the person with respect data fed in the PC using its arms. IR is used for person Identification. In the **MODIFICATION** that we propose is, once the user provides the voice input, the system will verify all the available books, and finds out the best book by comparing Input term frequency with total number of keywords extracted using Stemming Algorithm. So that resultant book shelf is identified by the Robot.

ALGORITHM / METHODOLOGY: Stemming, Ranking, Scoring

DOMAIN: Mobile Computing, Data Mining, Embedded

IEEE REFERENCE: IEEE Paper on Information and Communication Technologies, 2013





AADHITYAA INFOMEDIA SOLUTIONS

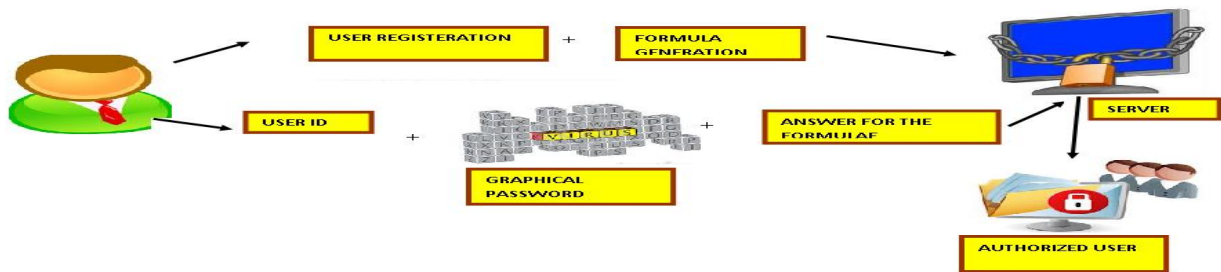
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10022 (JA 6031). A SIMPLE TEXT-BASED SHOULDER SURFING RESISTANT GRAPHICAL PASSWORD SCHEME

ARCHITECTURE DIAGRAM

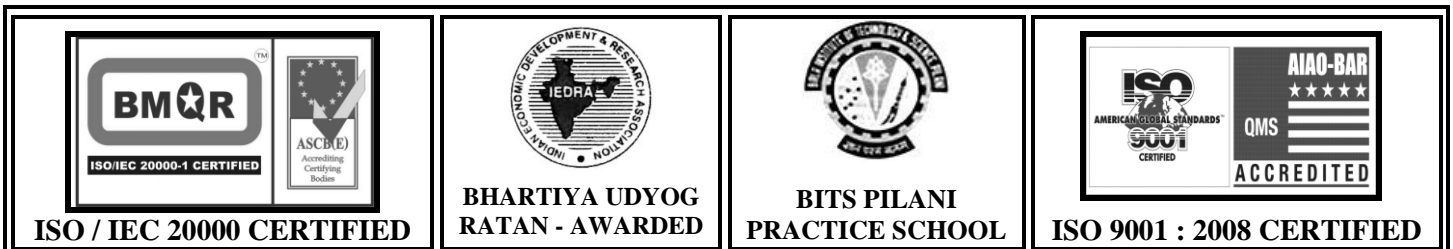


DESCRIPTION: In the **EXISTING SYSTEM**, we are only using textual password to login into our personal account such as Bank Account and Email Applications. These textual passwords are easily hacked by the attackers using Guessing attacks and Shoulder Surfing attacks. In the **PROPOSED SYSTEM**, we are implementing a Graphical Password Scheme in which, the User has to provide the User and Password in the Textual Manner and that will be saved in the Server for verification Process. While Login into the account, the User first enters their User Id, then they have to enter the password by using Graphical Scheme in which the alphabets and numbers are splitted into equal parts of different colors and the User have to find the each password letter is presented in the Graphical Region. Once the enters the Correct password, they are allowed to access the Application. In the **MODIFICATION PROCESS**, we also implement a formulae based Password Authentication Scheme in which the User can Choose the formulae while generating the password.

ALGORITHM / METHODOLOGY: Graphical Password Scheme

DOMAIN: Security

IEEE REFERENCE: IEEE Paper on Next Generation Electronics, 2013





AADHITYAA INFOMEDIA SOLUTIONS

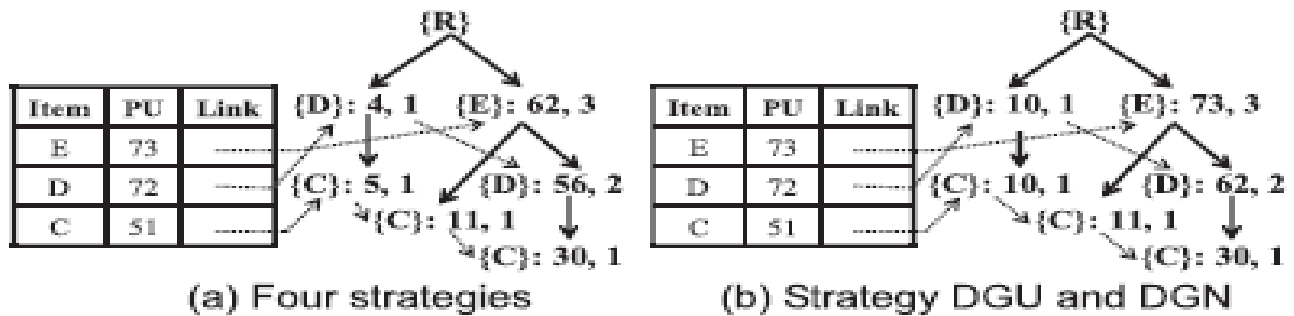
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10023 (NJA 15). EFFICIENT ALGORITHMS FOR MINING HIGH UTILITY ITEMSETS FROM TRANSACTIONAL DATABASES

ARCHITECTURE DIAGRAM

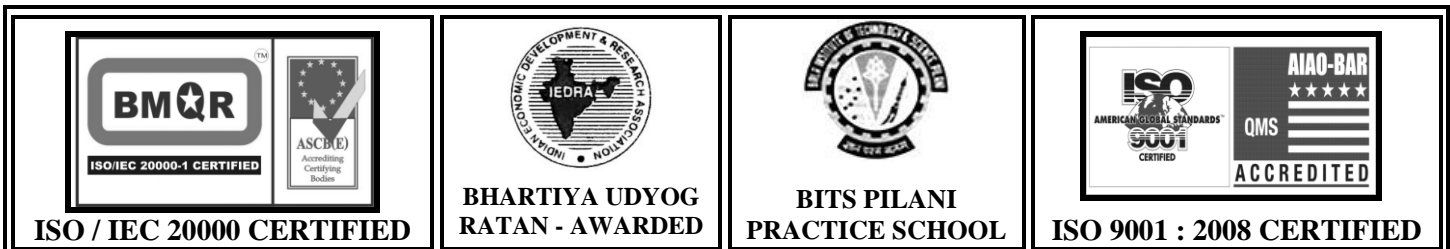


DESCRIPTION: In the **EXISTING SYSTEM**, In the framework of frequent item set mining, the importance of items to users is not considered. In the **PROPOSED SYSTEM**, User's interests of purchase of particular Products are monitored and Frequency Item set is extracted. Each node scan its local database and generates the frequent item sets using A-Priori algorithm then its corresponding gain value is computed. Based on this gain value, the high utility item sets are mined according to the user specified threshold send it to master node. In the **MODIFICATION**, we are measuring, follow up purchase of the set of Products from the date of purchase of first product. Ex User 1 would have purchased Computer, then 2 to 3 months later same user would purchase Printer. Wed can also measure Expected purchase of the set of products from the first purchase.

ALGORITHM / METHODOLOGY: IHUPTW

DOMAIN: Data Mining

IEEE REFERENCE: IEEE Transactions on Knowledge and Data Engineering, 2013





AADHITYAA INFOMEDIA SOLUTIONS

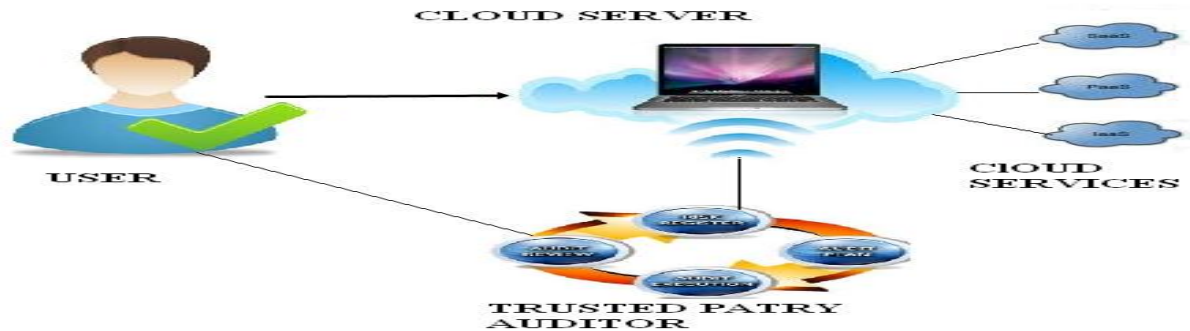
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10024 (NJA 17). MUTUAL BILLING VERIFICATION SYSTEM FOR DATA ACCESS IN CLOUD ENVIRONMENT

ARCHITECTURE DIAGRAM:






DESCRIPTION: In the **EXISTING SYSTEM**, Although Cloud Computing is vast developing technology, there is no trustworthiness and security for the data stored in the Cloud Servers. This lets people to avoid using Cloud Computing technology. In the **PROPOSED SYSTEM**, we introduce THEMIS, a new billing technology to use the services from the Cloud. By using THEMIS, each request and response of the Cloud Service providers and the User will send and monitored by Cloud Notary Authority. So that we can increase the trustworthiness of the Cloud Services. In the **MODIFICATION** process, we generating a session key and send as an SMS alert to the user’s mobile. Every time the user logs into the account, they’ve to enter the Username, Password and Session Key. If these things are authenticated, the user is allowed to access services of the Cloud. This will increase the security level.

ALGORITHM / METHODOLOGY: RANDON NUMBER GENERATION ALGORITHM

DOMAIN: Cloud Computing, Security

IEEE REFERENCE: IEEE TRANSACTIONS on Parallel and Distributed Systems, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



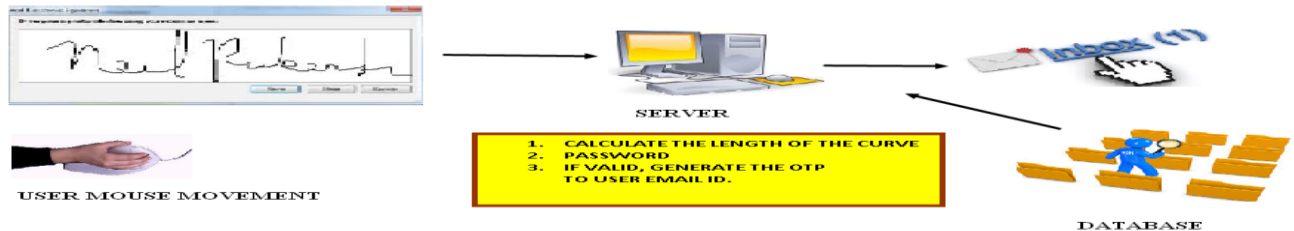
AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10025 (JA 6010). MOUSE BEHAVIOR BASED SIGNATURE AUTENTICATION USING NEURAL NETWORKS ARCHITECTURE DIAGRAM







DESCRIPTION: In the **EXISTING SYSTEM**, Recently, several large-scale password leakages exposed users to an unprecedented risk of disclosure and abuse of their information. the inadequacy of password-based authentication mechanisms is becoming a major concern for the entire information society. In the **PROPOSED SYSTEM**, consist of three major modules: (1) Mouse–Behavior Capture, (2) Feature Construction, and (3) Training / Classification. The first module serves to create a mouse-operation task, and to capture and interpret mouse-behavior data. The second module is used to extract holistic and procedural features to characterize mouse behavior and to map the raw features into distance-based features by using various distance metrics. The third module, in the training phase, applies neural network on the distance-based feature vectors to compute the predominant feature components, and then builds the user’s profile using a one-class classifier. In the classification phase, it determines the user’s identity using the trained classifier in the distance-based feature using NN. In the **MODIFICATION** process, a 4 Digit OTP is generated to the user’s email ID. The user will be giving the ‘2’ digit OTP and the server will be giving balance ‘2’ digit OTP. Users ‘2’ digit OTP is verified by the server and vice versa.

ALGORITHM / METHODOLOGY: Secure Random Number Generation, One-Class Learning Algorithm

DOMAIN: Security

IEEE REFERENCE: IEEE Transactions on Information Forensics and Security, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

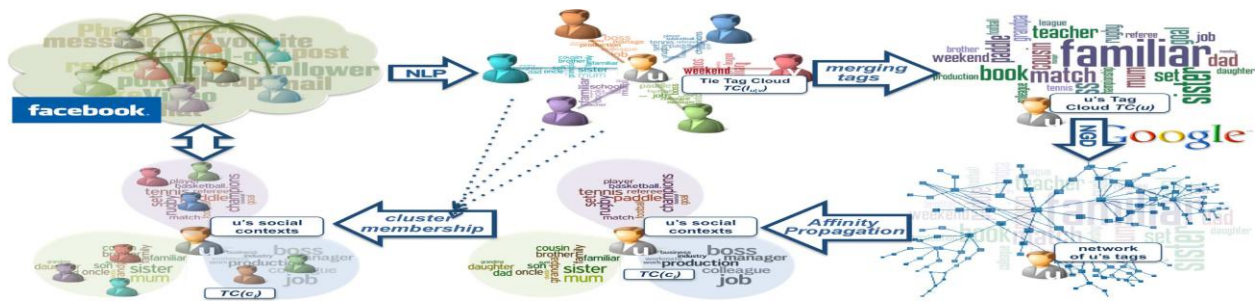
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10026 (NJA 19). INFERRING CONTEXTS FROM FACEBOOK INTERACTIONS: A SOCIAL PUBLICITY SCENARIO

ARCHITECTURE DIAGRAM



DESCRIPTION: The great acceptance of the Social Web has converted social networks, blogs and wikis in almost perfect advertising mediums. However, many of the current social publicity strategies do not exploit all the potential of these mediums, since they obviate users' online life: the social contexts in which they are involved. Our proposal to reverse this situation is a model to infer users' social contexts by the application of several Natural Language Processing (NLP) and data mining techniques over users' interaction data on Facebook. We take advantage of both Facebook and Groupon APIs to provide a deployment scenario in which knowing users' social life allows ads to target the most potential customers, which is beneficial for both companies and possible customers.

ALGORITHM / METHODOLOGY: Affinity Propagation algorithm

DOMAIN: Data Mining

IEEE REFERENCE: IEEE Transactions on Knowledge and Data Engineering, 2013



ISO / IEC 20000 CERTIFIED



BHARTIYA UDYOG
RATAN - AWARDED



BITS PILANI
PRACTICE SCHOOL



ISO 9001 : 2008 CERTIFIED



AADHITYAA INFOMEDIA SOLUTIONS

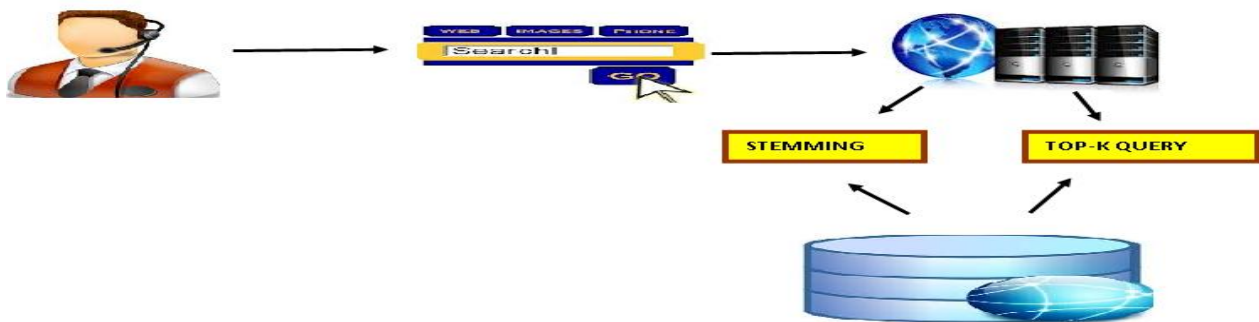
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10027 (JA 6023). AUTOMATIC CLASSIFICATION OF DOCUMENT CLUSTERING WITH BEST DATA RETRIEVAL SYSTEM USING SCORING & TOP K QUERY ALGORITHM

ARCHITECTURE DIAGRAM







DESCRIPTION: In the **EXISTING SYSTEM**. Finding the appropriate number of clusters to which documents should be partitioned is crucial in document clustering. In the **PROPOSED MODEL**, we are developing an automated system for both named and Un-named Documents based on the Clustering Algorithms. A new document is created is submitted to the User, whereby we apply stemming algorithm to remove the stop words. Based on the Scoring Algorithm, the documents are principally categorized into corresponding Clusters. As Per the Users request, the corresponding document is transferred to the User. In the **MODIFICATION PHASE** we also rank the best relevant documents based on Top K query for effective and efficient data retrieval system.

ALGORITHM / METHODOLOGY: Stemming Algorithm, Top K-Query Algorithm

DOMAIN: Data Mining

IEEE REFERENCE: IEEE Transactions on Knowledge and Data Engineering, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

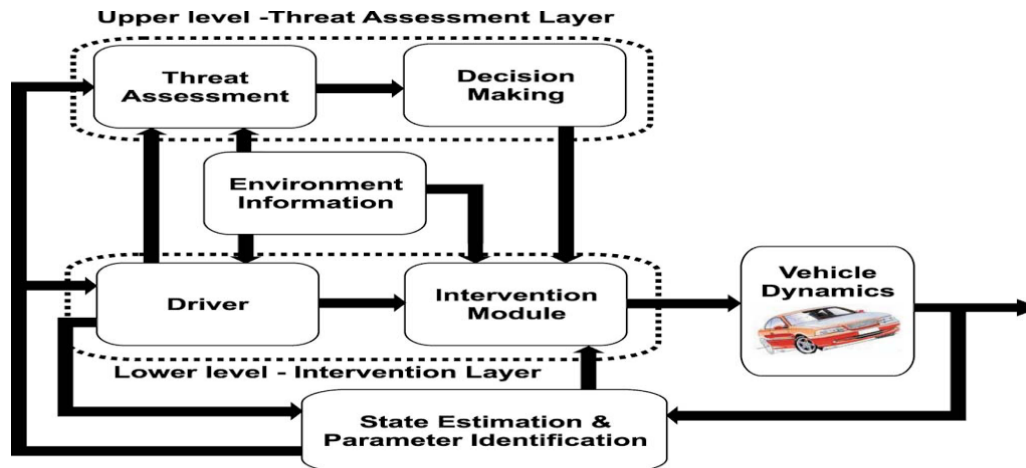
TRUST ME -
CRISIL
CERTIFIED

**(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)**



**DN 10028 (JA 6026). PROACTIVE ACCIDENT AVOIDANCE
SYSTEM FOR ROADSIDE VEHICLES**

ARCHITECTURE DIAGRAM







DESCRIPTION: In the **EXISTING SYSTEM**, there is no proper Predictive method to avoid the Traffic Accidents. .In the **PROPOSED SYSTEM**, If the owner is in the panic state and driving the without control in the steering, immediately an automatic control is provided to avoid the accident. Same way over speed would be automatically controlled. Ultrasonic Sensor is attached with the Vehicle to avoid the accidents. This Project is aimed to predictive to possible accidents, before it occurs. This Process is used to prevent those accidents. In **MODIFICATION** process, Eye Ball Sensor is attached to the vehicle, if driver sleeps, this sensor will detect the automatically apply brake in order to avoid Accident

ALGORITHM / METHODOLOGY: Novel Decision-Making, Model-Based Threat Assessment

DOMAIN: Mobile Computing, Embedded

IEEE REFERENCE: IEEE Transactions on Intelligent Transportation Systems, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
-----------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

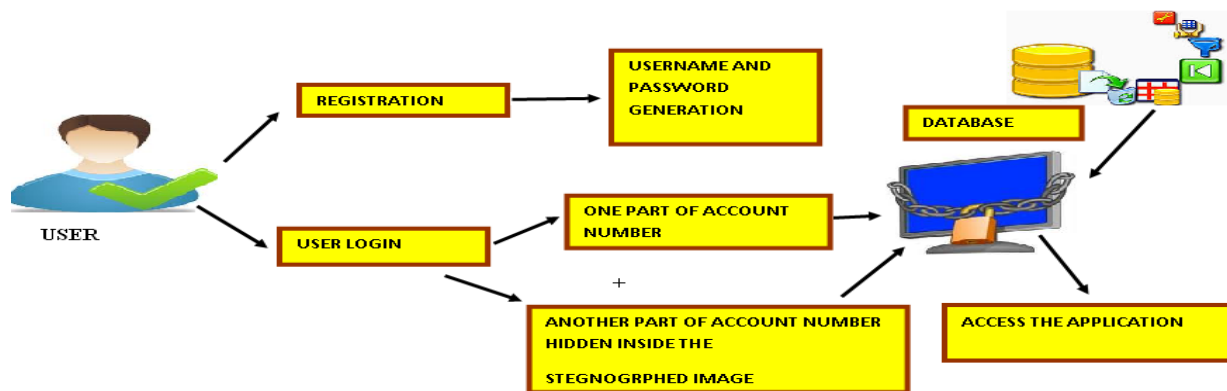
TRUST ME -
CRISIL
CERTIFIED

**(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)**



**DN 10029 (JA 6041). AVERTING MAN IN THE BROWSER
ATTACK USING USER-SPECIFIC PERSONAL IMAGES**

ARCHITECTURE DIAGRAM







DESCRIPTION: In the **EXISTING SYSTEM**, the text passwords are easily hacked by the Hackers. So lot of changes to perform many malicious activities. In the **PROPOSED SYSTEM**, User will be entering the Account Number for which amount is to be deposited. The Account Number is encrypted. The part of Encrypted data is send separately and other hidden in an image using Steganography and is send to the server. Server Destegnograph the image to extract the encrypted part of the Account Number and combines another part of Encrypted account number. Bother are Decrypted to form original Account Number on which Amount is credited.

ALGORITHM / METHODOLOGY:

DOMAIN: Security

IEEE REFERENCE: IEEE Paper on Advance Computing, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

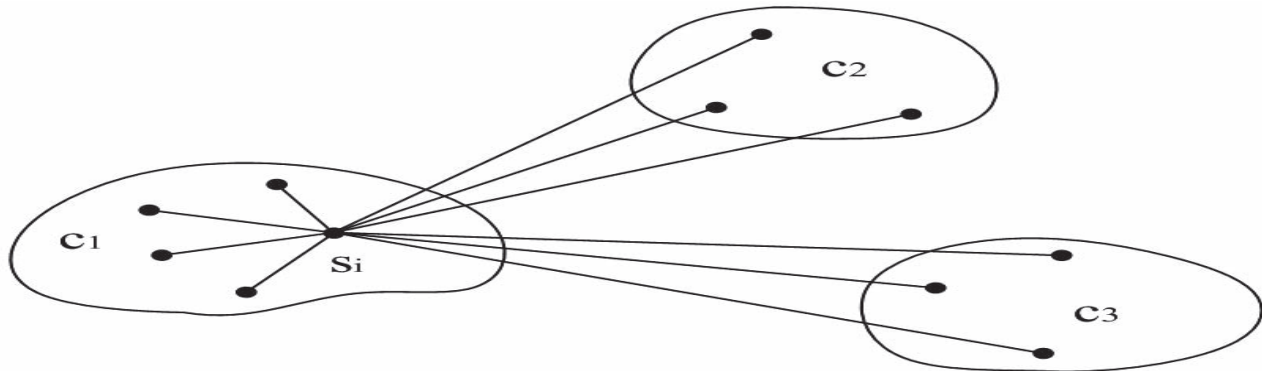
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10030 (JA 6049). DISA: MODELING AND DETECTION OF IP SPOOFING ATTACKS

ARCHITECTURE DIAGRAM



DESCRIPTION: In the **EXISTING SYSTEM**, spoofing attacks are easy to launch and can significantly impact the performance of networks. Although the identity of a node can be verified through cryptographic authentication, conventional security approaches are not always desirable because of their overhead requirements. In the **PROPOSED SYSTEM**, we are using three methods 1. Detection of Spoofing attacks 2. Determining the number of attackers when multiple adversaries masquerading the same node identity. 3. Localizing the multiple adversaries. In the **MODIFICATION PROCESS**, we are also encrypting the data packets during transmission for security purpose.

ALGORITHM / METHODOLOGY: Silence Mechanism

DOMAIN: Network Security

IEEE REFERENCE: IEEE Transactions on Parallel and Distributed system, 2013



ISO / IEC 20000 CERTIFIED



BHARTIYA UDYOG
RATAN - AWARDED



BITS PILANI
PRACTICE SCHOOL



ISO 9001 : 2008 CERTIFIED



AADHITYAA INFOMEDIA SOLUTIONS

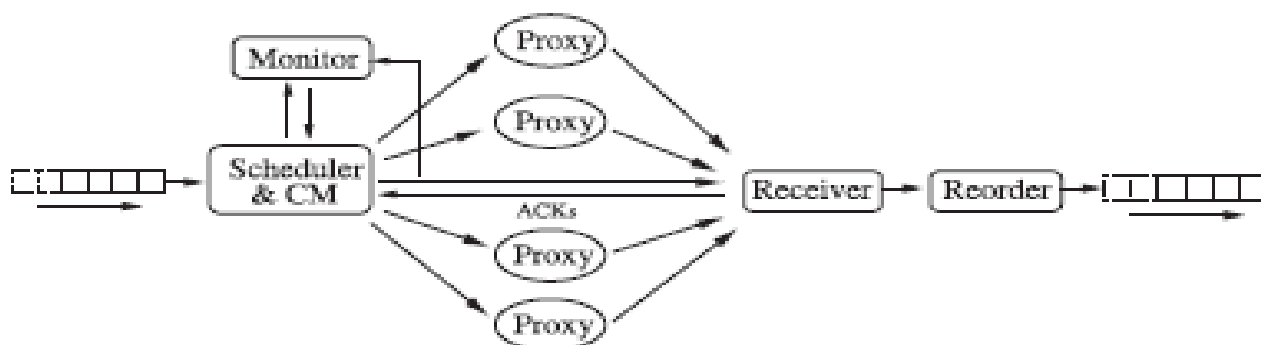
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10031 (NJA 20). MPATH: HIGH-BANDWIDTH DATA TRANSFERS WITH MASSIVELY MULTIPATH SOURCE ROUTING

ARCHITECTURE DIAGRAM





DESCRIPTION: The capacity of access links has increased dramatically in recent times, and bottlenecks are moving deeper into the Internet core. When bottlenecks occur in a core (or AS-AS peering) link, it is possible to use additional detour paths to improve the end to- end throughput between a pair of source and destination nodes. We propose and evaluate a new massively multipath (mPath) source routing algorithm to improve end-to-end throughput for high-volume data transfers. We demonstrate that our algorithm is practical by implementing a system that employs a set of proxies to establish one-hop detour paths between the source and destination nodes.

ALGORITHM / METHODOLOGY: Source Routing Algorithm

DOMAIN: Networking

IEEE REFERENCE: IEEE Transactions on Parallel and Distributed Systems, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

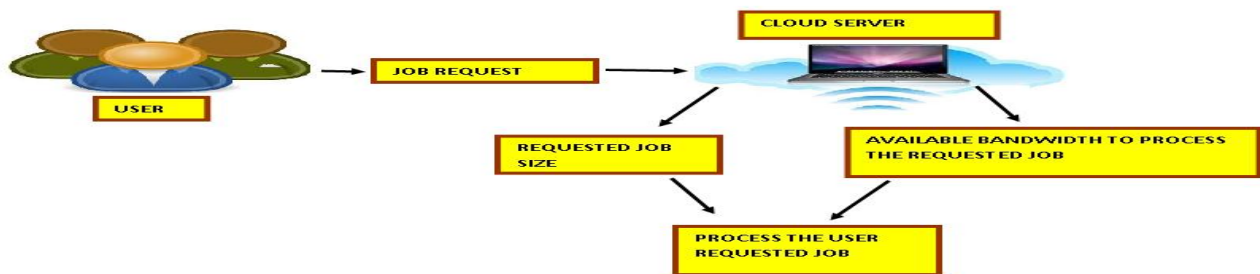
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10032 (JA 6009). DESIGN OF EFFECTIVE RESOURCE MANAGEMENT & SCHEDULING IN CLOUD NETWORK ENVIRONMENT.

ARCHITECTURE DIAGRAM







DESCRIPTION: In the **EXISTING SYSTEM**, the cloud computing paradigm is attracting an increased number of complex applications to run in remote data centers. Existing parallel scheduling mechanisms normally take responsiveness as the top priority and need nontrivial effort to make them work for data centers in the cloud era. In the **PROPOSED SYSTEM**, we propose a priority-based method to consolidate parallel workloads in the cloud. High Work Loaded is Assigned to the Maximum Resourced Machine. We Apply Two Algorithms namely, CMBF where space is incapable to perform a job in a server for a work but for another work it is feasible then second work is processed first and the first work is kept aside until the server becomes free. AMBF is the process by which all the available bandwidth is added to perform another work. In the **MODIFICATION** Part, User can specify the Priority of the Job and accordingly the work is performed as well as we calculated the available Resources to Perform the Work.

ALGORITHM / METHODOLOGY: CMBF, AMBF

DOMAIN: Networking

IEEE REFERENCE: IEEE TRANSACTIONS on Parallel and Distributed Systems, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

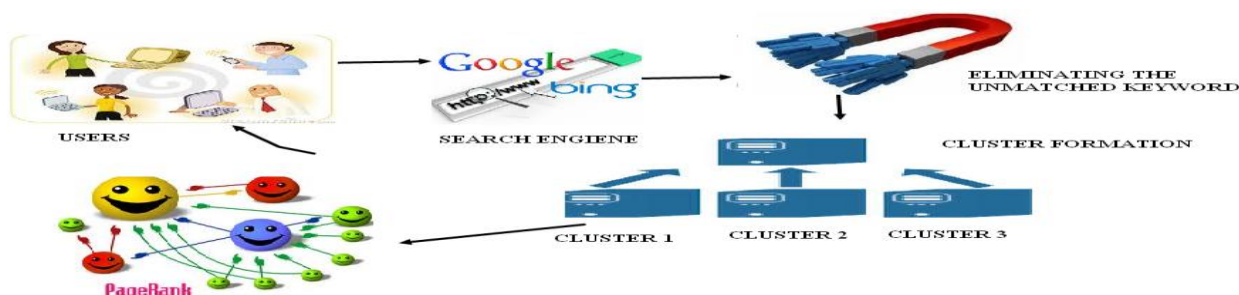
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10033 (JA 6038). MODELING SMARTY WEB SEARCH ENGINE USING XML CLUSTER

ARCHITECTURE DIAGRAM




DESCRIPTION: In the **EXISTING SYSTEM**, Searching is a very tedious Process because, we all be giving the different Keywords to the Search engine until we land up with the Best Results. There is no Clustering Approach is achieved in the Existing. In the **PROPOSED SYSTEM**, Feature selection involves identifying a subset of the most useful features that produces compatible results as the original entire set of features. The FAST algorithm works in two steps. In the first step, features are divided into clusters by using graph-theoretic clustering methods. In the second step, the most representative feature that is strongly related to target classes is selected from each cluster to form a subset of features. **MODIFICATION** is that XML based Cluster Formation is achieved in order to have Space and Language Competency.

ALGORITHM / METHODOLOGY: Fast Clustering-Based Feature Selection (FAST)

DOMAIN: Data Mining

IEEE REFERENCE: IEEE Transactions on Knowledge and Data Engineering, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

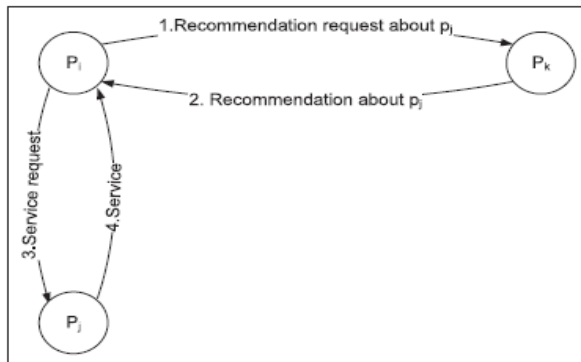
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10034 (JA 6065). DYNAMIC PEER TRUST AND LOAD MONITORING FOR EFFECTIVE DATA DELIVERY.

ARCHITECTURE DIAGRAM



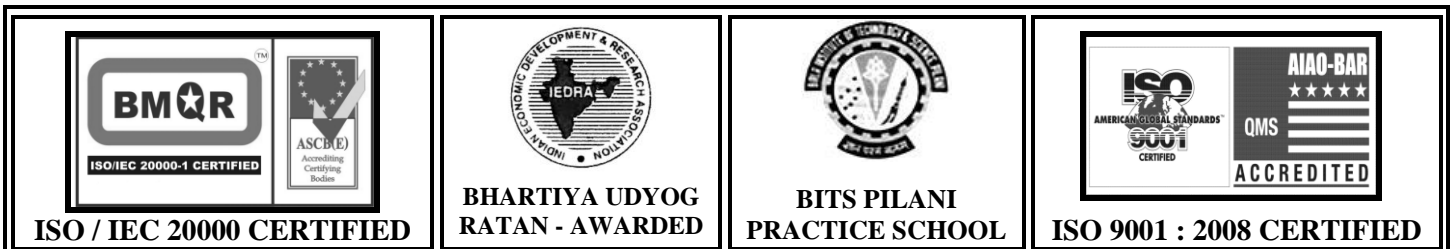
❖ **TRUSTWORTHINESS BASED ON PASSED INTERACTION AND RECOMMENDATIONS**

DESCRIPTION: In the **EXISTING SYSTEM**, due to the open nature of the Peer-to-Peer System can exposes them to malicious activity. In **PROPOSED SYSTEM**, we are calculating the trustworthiness of the peers based on the past interactions and recommendations. So that we can send the data safely. Also if a node wants a Service from other nodes (Multiple nodes providing the same Service) we can calculate the Service Metric level, Service History size. If both of them are equal, the Service requested node randomly chooses the Service Provider node. In the **MODIFICATION PROCESS**, if both the service providing nodes are having equal priority then we can calculate the loads of that nodes, so that the service requested node can get the service from the Service Provider node which having minimum load. So that the nodes can effectively process the other nodes requests.

ALGORITHM / METHODOLOGY: Load balancing Algorithm

DOMAIN: Network Security

IEEE REFERENCE: IEEE Transactions on Dependable and Secure Computing, 2013





AADHITYAA INFOMEDIA SOLUTIONS

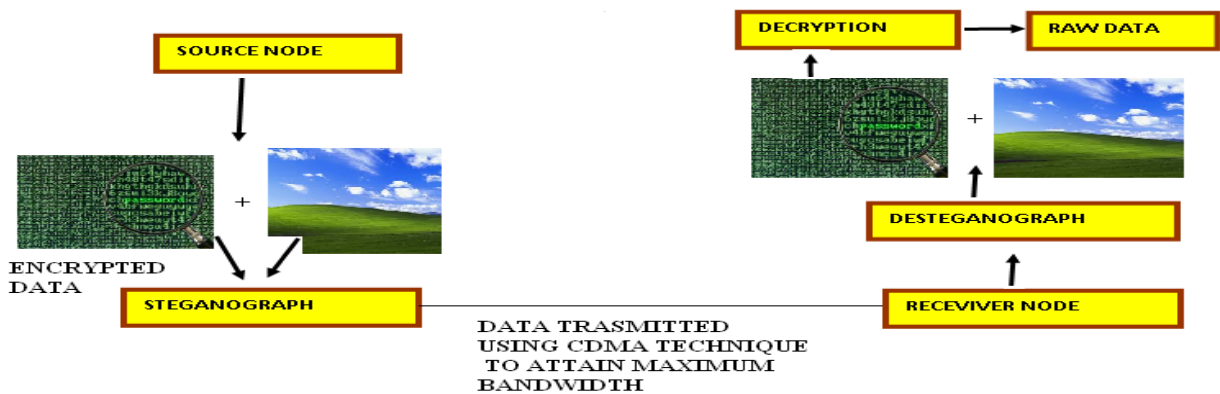
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10035 (JA 6013). SECURED DATA ENCRPTION AND STEGNOGRAPHY SYSTEM FOR EFFECTIVE COMMUNICATION USING SPREAD-SPECTRUM FROM DIGITAL MEDIA

ARCHITECTURE DIAGRAM:



DESCRIPTION: In the **EXISTING SYSTEM**, there is no big implementation was done, to protect that data are traveling via Wireless Network. In the **PROPOSED SYSTEM**, first we are Encrypting the Original data and Hide the Data into the image using Steganography mechanism. Then it will be transmitted to the Destination Node with maximum Speed. In the Destination Node, the Desteganograph Process will takes place, so that the original Image and Encrypted data is separated. Then the encrypted data will be decrypted using Decryption Algorithm.

ALGORITHM / METHODOLOGY: BSS Algorithm

DOMAIN: Image Processing

IEEE REFERENCE: IEEE Transactions on Secure Computing, 2013

<p>ISO / IEC 20000 CERTIFIED</p>	<p>BHARTIYA UDYOG RATAN - AWARDED</p>	<p>BITS PILANI PRACTICE SCHOOL</p>	<p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------	-------------------------------------------	----------------------------------------	----------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10036 (JA 6018). HIGH PERFORMANCE RESOURCE ALLOCATION STRATEGIES FOR COMPUTATIONAL ECONOMIES

ARCHITECTURE DIAGRAM





DESCRIPTION: In the **EXISTING SYSTEM**, Efficient Resource Allocation mechanism and effective Job processing was limited to the Lack of Performance and High Overhead. In the **PROPOSED SYSTEM**, first the Users Job request is passed to the Main Grid Server and the main Grid Server will Process the Job by allocating the Job to the Sub Server based five different Strategies name OverBooking, Just-In Time Bidding, Advanced Reservation, Two Phase Contract and Second Chance Substitute Providers. Based the User's selection the Concerned Server will Process the User requested Job. The Cost will be calculated based on the User Requested Strategy. The **MODIFICATION** that we propose in this Paper is to identify & Analyze the Required Resources to perform a Particular Requested Job with the available resources of various Servers in the Network. The Main Grid Server will list the Sub Servers which can perform the Requested Job to the User, so that the User can choose Suitable Sub Server.

ALGORITHM / METHODOLOGY: Scheduling Algorithm

DOMAIN: Grid Computing

IEEE REFERENCE: IEEE Transactions on Parallel and Distributed Systems, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

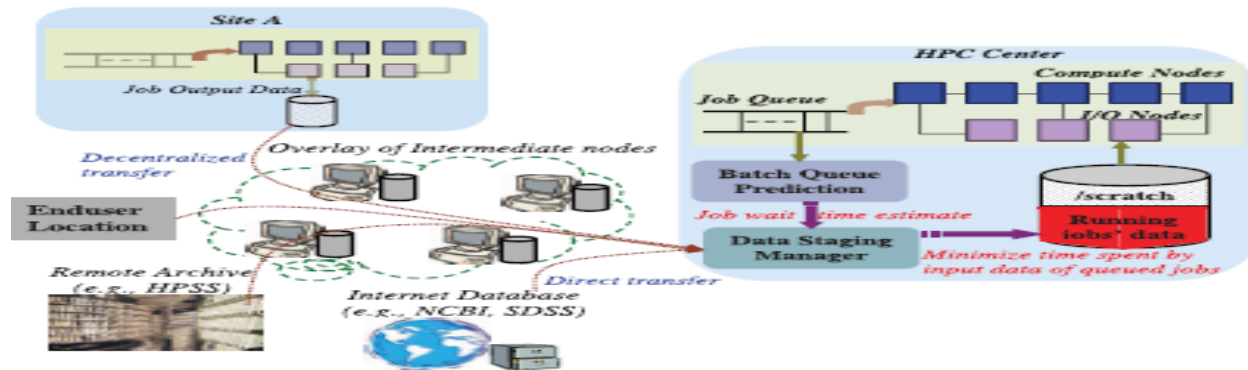
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10037. ON TIMELY STAGING OF HPC JOB INPUT DATA

ARCHITECTURE DIAGRAM







DESCRIPTION: Innovative scientific applications and emerging dense data sources are creating a data deluge for high-end supercomputing systems. Modern applications are often collaborative in nature, with a distributed user base for input and output data sets. Processing such large input data typically involves copying (or staging) the data onto the supercomputer's specialized high-speed storage, scratch space, for sustained high I/O throughput. This copying is crucial as remotely accessing the data while an application executes results in unnecessary delays and consequently performance degradation. However, the current practice of conservatively staging data as early as possible makes the data vulnerable to storage failures, which may entail restaging and reduced job throughput. To address this, we present a timely staging framework that uses a combination of job start-up time predictions, user-specified volunteer or cloud-based intermediate storage nodes, and decentralized data delivery to coincide input data staging with job start-up.

ALGORITHM / METHODOLOGY: Timely Staging

DOMAIN: Networking

IEEE REFERENCE: IEEE Transactions on Parallel and Distributed Systems, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED AIAO-BAR ACCREDITED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

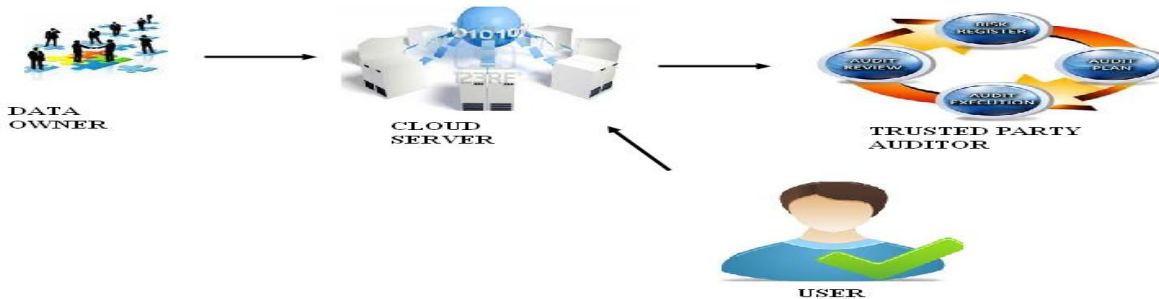
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10038 (JA 6032). ENSURING DATA RELIABILITY AND TRUST MANAGEMENT IN CLOUD ENVIRONMENT

ARCHITECTURE DIAGRAM



DESCRIPTION: In the **EXISTING SYSTEM**, there is no big implementation towards security for the data that are stored in the Cloud Server. So the trust worthiness to store the data in the cloud servers is decreased rapidly. In the **PROPOSED SYSTEM**, the data owner uploads the data in the Cloud server in encrypted format. The data in the Cloud Server will be hashed and the hashed values are given to the TPA for auditing purpose. The data will be audited by the TPA using the Merkle Hash Tree technique. If the data owner updates the data, the corresponding hash values are also updated. If the authorized user wants to access the data, they (user) have to provide the corresponding decryption key. In the **MODIFICATION** Process, while auditing the data, the TPA has to audit it from the IP address in which they (TPA) have registered. Accessing from any other system is not allowed.

ALGORITHM / METHODOLOGY: AES

DOMAIN: Cloud Computing, Security

IEEE REFERENCE: IEEE Transactions on Dependable and Secure Computing, 2013

<p>ISO / IEC 20000-1 CERTIFIED</p>	<p>BHARTIYA UDYOG RATAN - AWARDED</p>	<p>BITS PILANI PRACTICE SCHOOL</p>	<p>ISO 9001 : 2008 CERTIFIED</p>
------------------------------------	-------------------------------------------	----------------------------------------	----------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

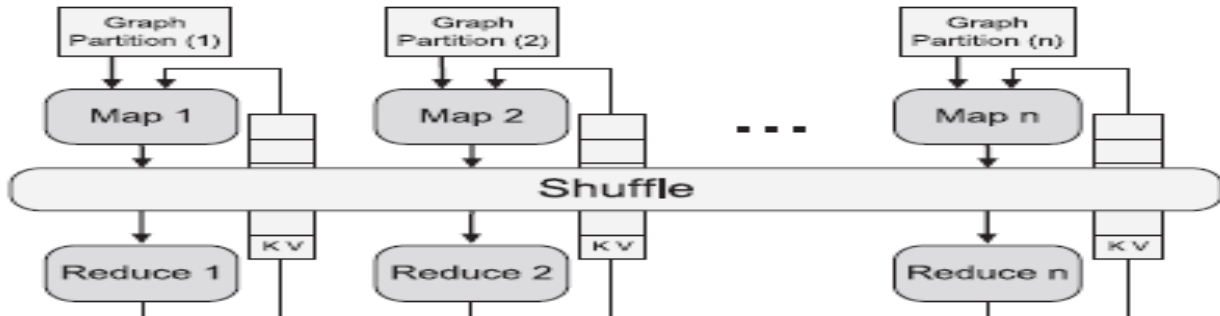
TRUST ME -
CRISIL
CERTIFIED

**(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)**



**DN 10039 (JA 6033). PRITER: A DISTRIBUTED FRAMEWORK
FOR PRIORITIZING ITERATIVE COMPUTATIONS**

ARCHITECTURE DIAGRAM






DESCRIPTION: Iterative computations are pervasive among data analysis applications, including web search, online social network analysis, recommendation systems, and so on. These applications typically involve data sets of massive scale. Fast convergence of the iterative computations on the massive data set is essential for these applications. In this paper, we explore the opportunity for accelerating iterative computations by prioritization. Instead of performing computations on all data points without discrimination, we prioritize the computations that help convergence the most, so that the convergence speed of iterative process is significantly improved. We develop a distributed computing framework, PrIter, which supports the prioritized execution of iterative computations. PrIter either stores intermediate data in memory for fast convergence or stores intermediate data in files for scaling to larger data sets.

ALGORITHM / METHODOLOGY: Support Vector Machine (SVM)

DOMAIN: Web, Networking

IEEE REFERENCE: IEEE Transactions on Parallel and Distributed Systems, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

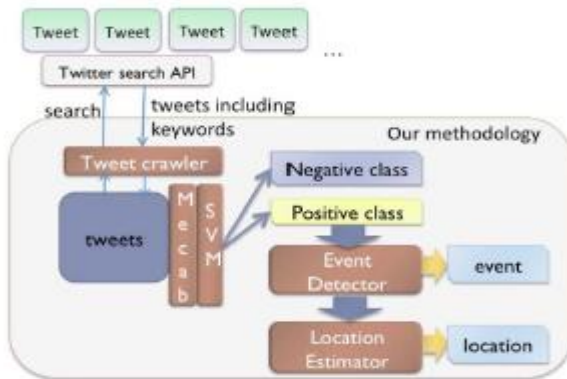
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10040 (JA 6034). IMPLEMENTATION OF SPEEDY EMERGENCY ALERT USING TWEET ANALYSIS

ARCHITECTURE DIAGRAM



SVM Features of an Example Sentence

Feature Name	Features
Features A	7 words, the fifth word
Features B	I, am, in, Japan, earthquake, right, now
Features C	Japan, right

DESCRIPTION: In the **EXISTING SYSTEM**, there is no proper alert system was implemented to report about the earthquake, so there is no way to take immediate rescue process to save the people. In the **PROPOSED MODEL**, we use particle filter. This model extracts the important keywords from tweets using Stemming along with the location and time. If the system interfaces Maximum Peak of the particular keyword like "Earthquake / Typhoon / Tsunami" at a particular time and at particular location, a peak is generated immediately an auto alert is passed to the nearest people present in the nearest location as emergency alert. In the **MODIFICATION** process, an emergency alert is send as Sms and E-mail alert for the registered tweet users as well as to the Nearest Rescue Team.

ALGORITHM / METHODOLOGY: Support Vector Machine (SVM)

DOMAIN: Data Mining

IEEE REFERENCE: IEEE Transactions on Knowledge and Data Engineering, 2013

<p>ISO / IEC 20000 CERTIFIED</p>	<p>BHARTIYA UDYOG RATAN - AWARDED</p>	<p>BITS PILANI PRACTICE SCHOOL</p>	<p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------	-------------------------------------------	----------------------------------------	----------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

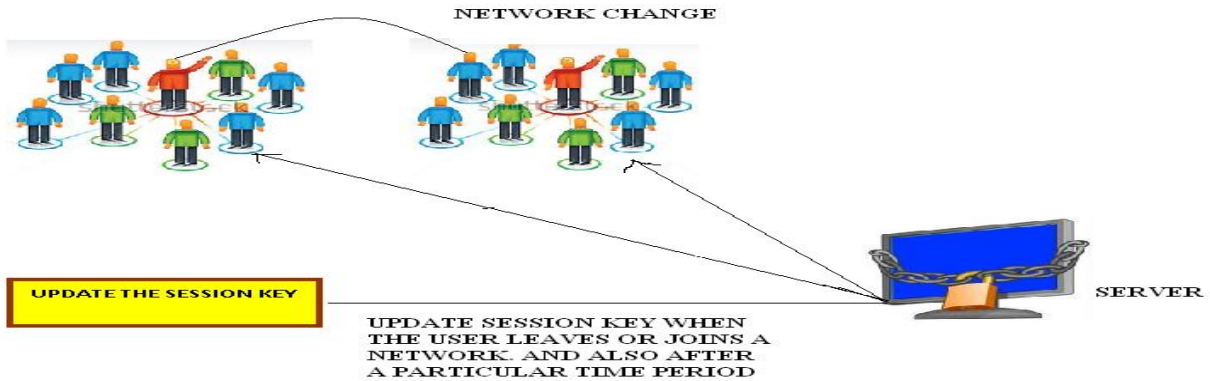
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10041 (JA 6037). DYNAMIC KEY FOR SECURED COMMUNICATION AMONG THE FLEXIBLE NODES

ARCHITECTURE DIAGRAM



DESCRIPTION: In the **EXISTING SYSTEM**, there is no proper security measures were implemented in Wireless Ad-hoc Networks while joining new nodes and exchanging data. In the **PROPOSED SYSTEM**, if a new node want to with the existing node, the new node will send the request to the existing node. Based on the request, the existing node will send its public key to the new node. After that the new node and existing node will share their public and private key components to authenticate each other. For security purpose the data will be Encrypted during transmission. The Certificate Authority is used to authorize the node when it wants joins another node. Secret key is generated, which is used to share the data and it will be changed at a particular period of time. In the **MODIFICATION** process, the secret key is also changed when the node joins a network and leaves a network. So that we can increase the level of security.

ALGORITHM / METHODOLOGY: AES, RSA

DOMAIN: Wireless Ad-hoc Networks

IEEE REFERENCE: IEEE Transactions on Parallel and Distributed Systems, 2013



ISO / IEC 20000 CERTIFIED



BHARTIYA UDYOG
RATAN - AWARDED



BITS PILANI
PRACTICE SCHOOL



ISO 9001 : 2008 CERTIFIED



AADHITYAA INFOMEDIA SOLUTIONS

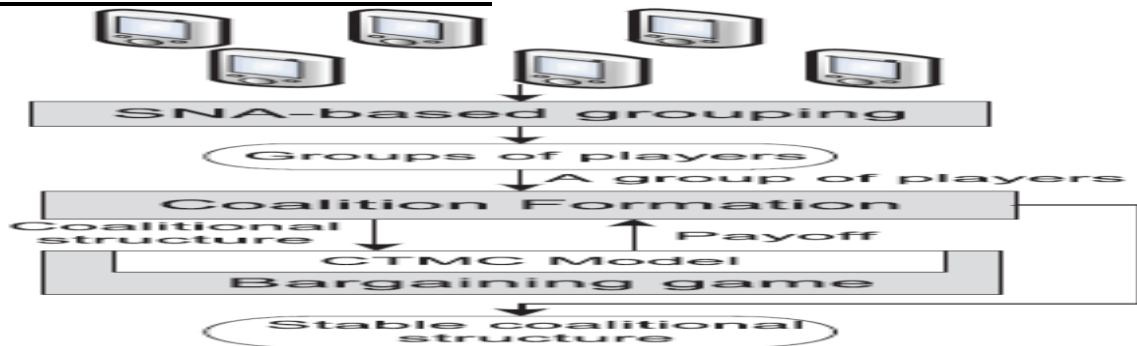
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10042 (JA 6040). BPO: ASSURED CO-OPERATIVE PACKET DELIVERY IN WIRELESS MOBILE NETWORKS USING COALITIONAL GAME AND BEST PAYOFF APPROACH

ARCHITECTURE DIAGRAM



DESCRIPTION : In the **EXISTING SYSTEM**, Mobile Nodes (e.g., vehicles) in the same group for Data Exchange is always very difficult, Costly, Time Delay in Delivery. We consider the problem of cooperative packet delivery to mobile nodes in a hybrid wireless mobile network. In the **PROPOSED SYSTEM**, a solution is deployed based on a coalition formation among mobile nodes to cooperatively deliver packets among these mobile nodes in the same coalition. Mobile nodes make a decision to join or to leave a coalition based on their individual payoffs. The individual payoff of each mobile node is a function of the average delivery delay for packets transmitted to the mobile node from a base station and the cost incurred by this mobile node for relaying packets to other mobile nodes. Markov chain model is formulated and the expected cost and packet delivery delay. A bargaining game is used to find the optimal helping probabilities. In the **MODIFICATION PROCESS**, Trustworthiness along with the Payoff of a Mobile Node is also considered before forwarding a Data to any Mobile Node.

ALGORITHM / METHODOLOGY: SNA BASED ALGORITHM

DOMAIN: Mobile Computing

IEEE REFERENCE: IEEE Transactions on Mobile Computing, 2013



ISO / IEC 20000 CERTIFIED



BHARTIYA UDYOG
RATAN - AWARDED



BITS PILANI
PRACTICE SCHOOL



ISO 9001 : 2008 CERTIFIED



AADHITYAA INFOMEDIA SOLUTIONS

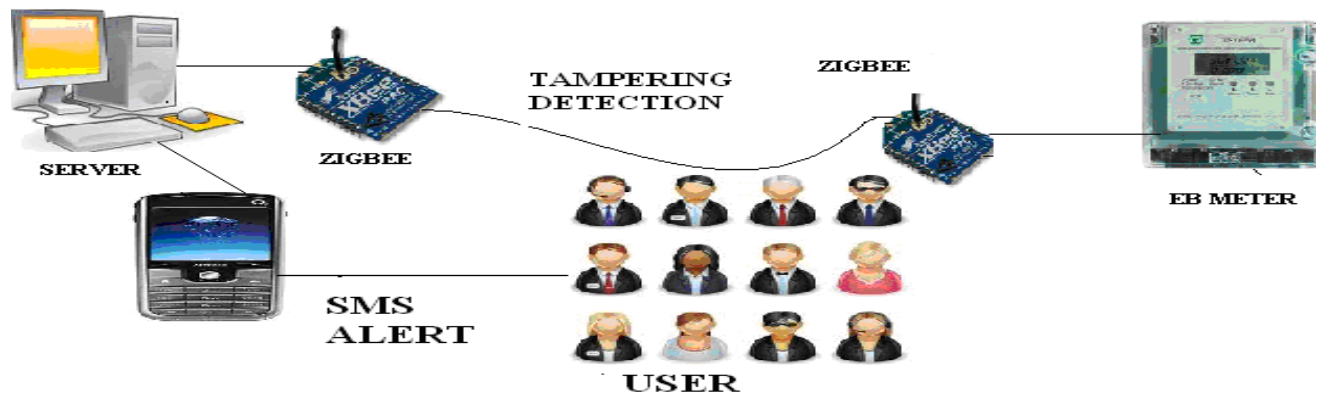
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10043 (JA 6044). DESIGN OF WIRELESS SENSOR BASED AUTOMATIC METER READING WITH TAMPERING DETECTION

ARCHITECTURE DIAGRAM







DESCRIPTION: In the **EXISTING SYSTEM**, Traditional electro-mechanical meters, still Widely used today, are prone to drift over temperature and time. EB Person has to come home and take the Meter Readings manually. In the **PROPOSED SYSTEM**, GSM network is used to detect the EB Meter Readings and Automatic SMS Alert is send to the Customer. In the **MODIFICATION** Part, We implement Zigbee Technology instead of GSM as it is cheaper and will be useful even Not Reachable Tower Accessibility Areas also. One Zigbee is connected to the EB Server and another is connected to the Home EB Meter. EB Meter Readings are obtained using Zigbee Network as well we are detecting Neutral Tampering

ALGORITHM / METHODOLOGY:

DOMAIN: Embedded, Security

IEEE REFERENCE: IEEE Paper on Automation Computing and Compression Sensing, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

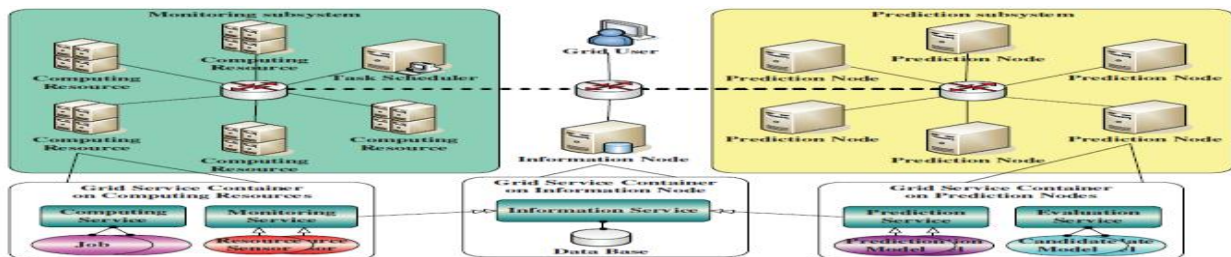
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10044 (JA 6066). PERFORMANCE-DRIVEN LOAD BALANCING WITH A BACKUP APPROACH FOR COMPUTATIONAL GRIDS WITH LOW COST

ARCHITECTURE DIAGRAM:

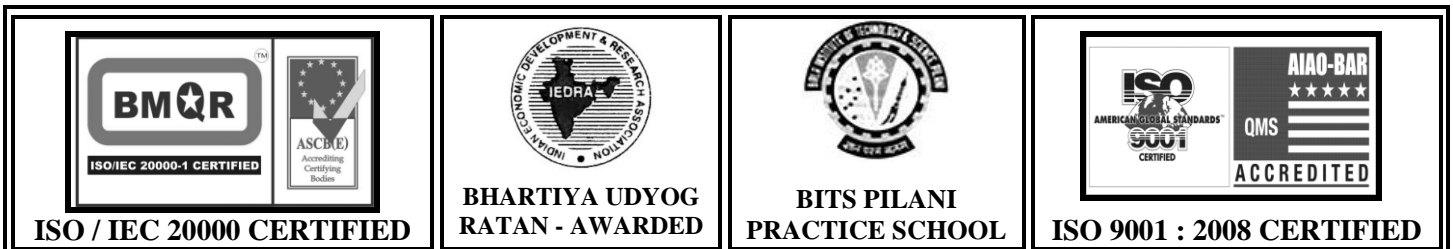


DESCRIPTION: Computational grids provide a massive source of processing power, providing the means to support processor intensive applications. The strong burstiness and unpredictability of the available resources raise the need to make applications robust against the dynamics of grid environment. The two main techniques that are most suitable to cope with the dynamic nature of the grid are load balancing and job replication. In this work, we develop a load-balancing algorithm by juxtaposes the strong points of neighbor-based and cluster-based load-balancing methods. We then integrate the proposed load-balancing approach with fault-tolerant scheduling namely MinRC and develop a performance-driven fault-tolerant load-balancing algorithm or PD_MinRC for independent jobs. In order to improve system flexibility, reliability, and save system resource, PD_MinRC employs passive replication scheme. Our main objective is to arrive at job assignments that could achieve minimum response time, maximum resource utilization, and a well-balanced load across all the resources involved in a grid.

ALGORITHM / METHODOLOGY: Load balancing Algorithm

DOMAIN: Grid Computing, Security

IEEE REFERENCE: IEEE Transactions on Dependable and Secure Computing, 2013





AADHITYAA INFOMEDIA SOLUTIONS

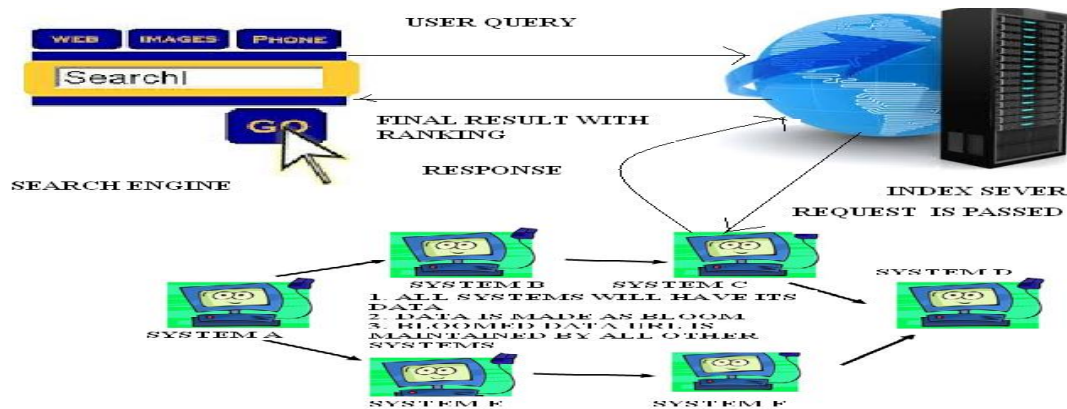
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10045 (JA 6055). DESIGN OF SPEEDY RETRIVAL SYSTEM USING BLOOM FILTER

ARCHITECTURE DIAGRAM



DESCRIPTION: In the **EXISTING SYSTEM**, Single Keyword based Approach is used to be Mapped with the Set of Document in the Nodes. In the **PROPOSED MODEL** Multi Keyword Search is Applied Where lots of Virtual Server is Deployed with Index Information of all the Documents. Peers will contain the Documents. Search is posted to Index Server Which Manages the Address Space of Virtual Server and Identifies the Data Contains Peer List. Best Records are Retrieved Using Ranking Process.

ALGORITHM / METHODOLOGY: Bloom Filter, Stemming, Ranking, Scoring

DOMAIN: Data Mining

IEEE REFERENCE: IEEE TRANSACTIONS on Systems, Man And Cybernetics: Systems, 2013



ISO / IEC 20000 CERTIFIED



BHARTIYA UDYOG
RATAN - AWARDED



BITS PILANI
PRACTICE SCHOOL



ISO 9001 : 2008 CERTIFIED



AADHITYAA INFOMEDIA SOLUTIONS

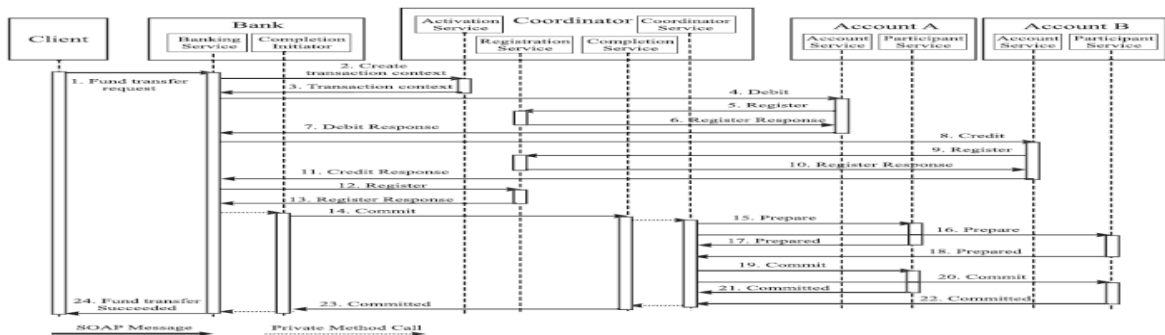
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10046 (JA 6059). EFFECTIVE IMPLEMENTATION OF TRUST WORTHY CO ORDINATION IN INTER COMMUNICATION WEB SERVER TRANSACTIONS

ARCHITECTURE DIAGRAM



DESCRIPTION: We present a lightweight Byzantine fault tolerance (BFT) algorithm, which can be used to render the coordination of web services business activities (WS-BA) more trustworthy. The lightweight design of the BFT algorithm is the result of a comprehensive study of the threats to the WS-BA coordination services and a careful analysis of the state model of WS-BA. The lightweight BFT algorithm uses source ordering, rather than total ordering, of incoming requests to achieve Byzantine fault tolerant, state-machine replication of the WS-BA coordination services. We have implemented the lightweight BFT algorithm, and incorporated it into the open-source Kandula framework, which implements the WS-BA specification with the WS-BA-I extension.

ALGORITHM / METHODOLOGY: Practical Byzantine Fault Tolerance Algorithm

DOMAIN: Web Services

IEEE REFERENCE: IEEE Transactions on Service Computing, 2013

<p>ISO / IEC 20000 CERTIFIED</p>	<p>BHARTIYA UDYOG RATAN - AWARDED</p>	<p>BITS PILANI PRACTICE SCHOOL</p>	<p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------	---------------------------------------	------------------------------------	----------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

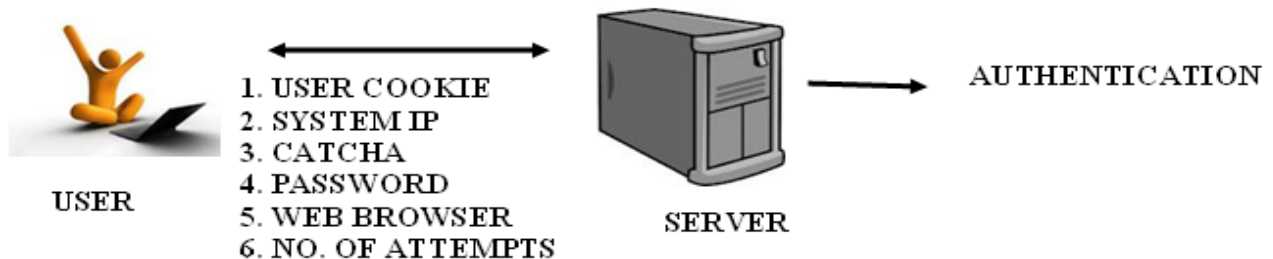
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10047 (JA 6067). DESIGN OF ONLINE USER IDENTIFICATION WITH MULTI LAYER DETECTION PROTOCOL

ARCHITECTURE DIAGRAM







DESCRIPTION: In the **EXISTING MODEL**, online Guessing attacks on Password Based Systems are inevitable and commonly observed against Web Applications. In the **PROPOSED SYSTEM**, the Server Verifies (1) User Name from the Cookie of the User's Machine, (2) System IP, (3) Capcha, (4) Password of the User, (5) Number of Failure Attempts by the User, (6) Web Browser that the User Uses for Browsing. This Process of Verification is called as Automated Turing Tests (ATT). The **MODIFICATIONS** that we Propose from the IEEE Base Paper is the Authentication of User by asking Secret Questions which was answered during the Registration Phase.

ALGORITHM / METHODOLOGY: Automated Turning Test

DOMAIN: Network Security

IEEE REFERENCE: IEEE Paper on Information Communication and Embedded Systems, 2013

 <p>ISO / IEC 20000-1 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

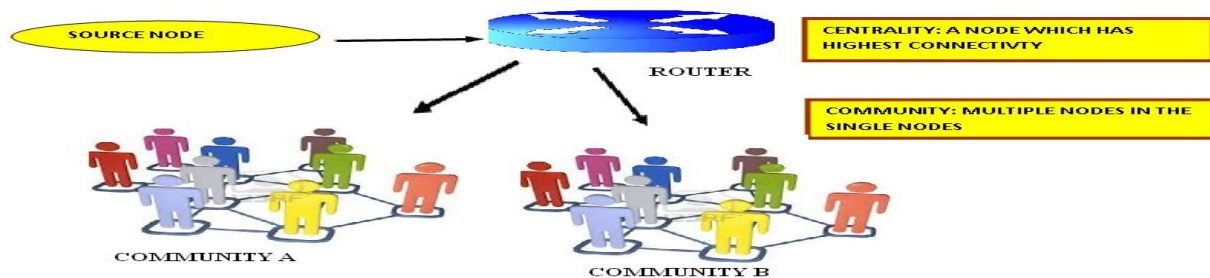
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10048 (JA 6068). IMPLEMENTATION OF EFFECTIVE DATA FORWARDING USING SOCIAL CONTACT PATTERNS IN MOBILE COMPUTING DTN ENVIRONMENT

ARCHITECTURE DIAGRAM







DESCRIPTION: In the **EXISTING SYSTEM**, Unpredictable node mobility, low node density, and lack of global information make it challenging to achieve effective data forwarding in Delay-Tolerant Networks (DTNs). Most of these nodes may not be the best relay choices within a short time period due to the heterogeneity of transient node contact characteristics. In the **PROPOSED SYSTEM**, a novel approach to improve the performance of data forwarding using Two Approaches, 1. Centrality 2. Community. Centrality deals by identifying a node which has Highest Connectivity with other nodes, so this centrality node can definitely deliver the data to the Destination without loss. In the Community Approach, is to find out a Community of Nodes formation where the destination is attached with, so that the data can be delivered to the Destination within the Short Period of time without Loss. The **MODIFICATION** that we propose is the security part, thereby we can encrypt the data & can be send to destination safely.

ALGORITHM / METHODOLOGY: Contact Patterns, Community

DOMAIN: Mobile Computing

IEEE REFERENCE: IEEE Transactions on Mobile computing, 2013

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------



AADHITYAA INFOMEDIA SOLUTIONS

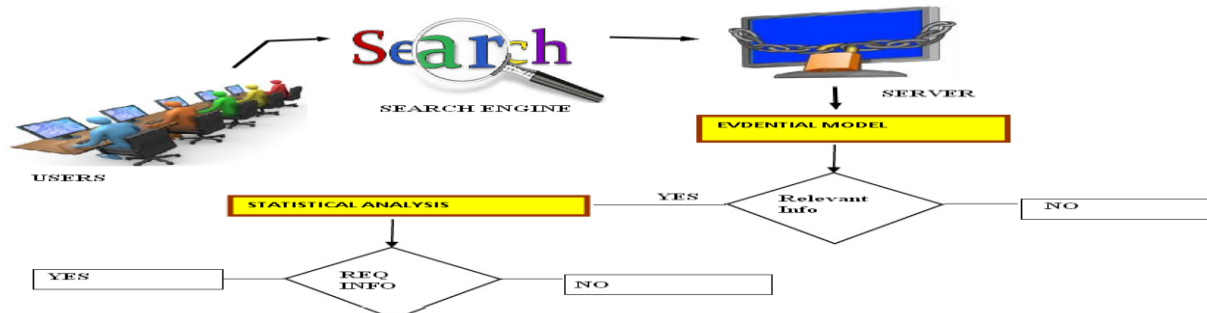
TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10049 (JA 6069). ORGANIZING AND RETRIVAL OF BEST RANKED LINKS USING USER FEEDBACK MODEL.

ARCHITECTURE DIAGRAM



DESCRIPTION: In the **EXISTING SYSTEM**, User gives the Search input to the Search Engine, which provides all sets of data irrespective of Relevant Results with respect to the Query as well as Redundant Results. In the **PROPOSED SYSTEM**, We are using Statistical and Evidence Approach to retrieve the Results. Statistical Approach is used in reranking the results after obtaining the Feedbacks from the different Users in the corresponding URLs. In the Evidence Approach, we are evaluating resultant URLs are really matched to the query, only then the resultant URLs are displayed to the user. **MODIFICATION** that we Propose is to get the Feedback of Rating for both the Key word Matched data as well as Information in the Resultant Data. This Process filters unwanted Resultant and provides Exactly Matched as well as Best Resultant Data to the users.

ALGORITHM / METHODOLOGY: Statistical and Evidence Algorithm

DOMAIN: Data Mining

IEEE REFERENCE: IEEE Transactions on Knowledge and Data Engineering, 2013



ISO / IEC 20000 CERTIFIED



BHARTIYA UDYOG
RATAN - AWARDED



BITS PILANI
PRACTICE SCHOOL



ISO 9001 : 2008 CERTIFIED



AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10050 (AJA 4). EFFECTIVE CLUTERING TECHNIQUE IN INFERRING BEST RESULTS USING USER’S FEEDBACK

In the **EXISTING SYSTEM**, it is so difficult to get the relevant information for the query we have entered. In the **PROPOSED SYSTEM**, novel approach to infer user search goals by analyzing search engine query logs. Once the User entered the query, the Resultant URLs will be filtered and the Pseudo-Documents are generated. Once the Pseudo documents are generated the Server will apply the Clustering Mechanism to URL’s. So that the URLs are listed as different Categories.

ALGORITHM / METHODOLOGY: Clustering

DOMAIN: Data Mining

IEEE REFERENCE: IEEE Transactions on Knowledge and Data Engineering, 2013

DN 10051. DESIGN OF VIRTUALIZATION AND LOAD MONITORING IN CLOUD

In the **EXISTING SYSTEM**, each Cloud Computing User (CCU) requests Cloud Computing Service Provider (CCSP) for use of resources. If CCU finds the server busy, then the user has to wait till the current user completes the job. This may result in increase of queue length as well as waiting time, which may lead to request drop. In the **PROPOSED SYSTEM**, we use a finite Multi Server Queuing Model with Queue Dependent heterogeneous servers where the applications are modeled as queues and the virtual machines are modeled as Service Providers. Request from the User is send to the CSP, where Dispatcher Pool will Redirect to Queue 1 or 2 alternatively and Throughput is calculated in the Virtual Machines for effective Data Processing. In the **MODIFICATION PROCESS**, We assign priority Model for Processing Important Data based High / Medium / Low Priority Model.

ALGORITHM / METHODOLOGY: Placement, Load Balancing

DOMAIN: Cloud Computing

IEEE REFERENCE: IEEE Transactions on Parallel and Distributed Systems, 2013



ISO / IEC 20000 CERTIFIED



BHARTIYA UDYOG
RATAN - AWARDED



BITS PILANI
PRACTICE SCHOOL



ISO 9001 : 2008 CERTIFIED



AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -
CRISIL
CERTIFIED

**(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)**



IEEE 2012 PROJECT LIST

DN 10052. IDENTIFICATION, DETECTION AND REMOVAL OF INTRUSION ATTACKS IN MULTITIER WEB APPLICATIONS

DOMAIN: Network Security

DN 10053. PREVENTION OF DDOS ATTACKS USING PORT NUMBER REVOLUTIONIZE & TIME STAMP – CLOCK DRIFTS

DOMAIN: Network Security

DN 10054. AUTONOMOUS SPECTRUM HANDOFF FRAMEWORK IN ADHOC NETWORK WITH DYNAMIC LOAD BALANCING

DOMAIN: Mobile Computing

DN 10055. IDENTIFICATION OF MALICIOUS PACKET LOSS DURING ROUTING MISBEHAVIOUR IN DTN

DOMAIN: Network Security



ISO / IEC 20000 CERTIFIED



BHARTIYA UDYOG
RATAN - AWARDED



BITS PILANI
PRACTICE SCHOOL



ISO 9001 : 2008 CERTIFIED



AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -
CRISIL
CERTIFIED

(FIRST (1ST) ISO 20000, SEI CMMI LEVEL 3
COMPLIANCE & ISO 9001 : 2008 CERTIFIED
SOFTWARE DEVELOPMENT COMPANY)



DN 10056. SECURED DATA SHARING WITH ACCESS PRIVILEGE POLICIES & DISTRIBUTED ACCOUNTABILITY IN CLOUD

DOMAIN: Cloud Computing, Security

DN 10057. DATA HIDING AND SECURED DATA STORAGE WITH ACCESS CONTROL TOWARDS MULTIPARTY PROTOCOLS

DOMAIN: Data Mining, Security





DN 10058. DETECTION AND FILTERING SPAMS WITH CONTENT, EXTENSION AND ACTIVITY MONITORING

DOMAIN: Network Security

DN 10059. A MACHINE BASED ANALYTIC APPROACH WITH SVM CLASSIFIER FOR FILTERING MOVIE AND PRODUCT QUALITY USING ANDROID SMART PHONE

DOMAIN: Mobile Computing, Android, Data Mining

YOUR OWN IDEAS ALSO

 <p>ISO / IEC 20000 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
----------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------