



# AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -  
CRISIL  
CERTIFIED

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



## PROJECTS IN JAVA / J2EE / J2ME / ANDROID

### IEEE PROJECTS 2013

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

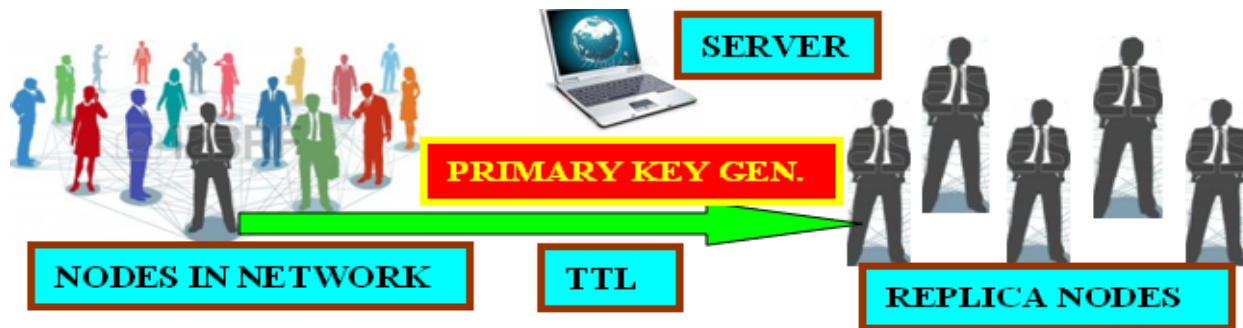
TRUST ME -  
CRISIL  
CERTIFIED

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



## NJA 2 (DN 10014). 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 (1<sup>ST</sup>) ISO 20000, SEI CMMI LEVEL 3  
COMPLIANCE & ISO 9001 : 2008 CERTIFIED  
SOFTWARE DEVELOPMENT COMPANY)



## NJA 3. REAL-TIME ANDROID BASED INDOOR NAVIGATION AND AUTOMATIC LOCATION ALERTING SYSTEM

### ARCHITECTURE DIAGRAM



1. Mobile User can make query from current place to the desired destination from their Android Mobile. Current Place is identified via Blue tooth.
2. Android application also intimates intermediate Departments during mobile user transit. User can fix appointments in the corresponding departments from Android and also can reach the destination parallely.

**DESCRIPTION :** In the **EXISTING SYSTEM**, Tracking of Indoor navigation is really tough and it is not achieved using GPS. In the **PROPOSED MODEL**, Android Mobile User can get the current location which is used to find the destination path. User can search the destination and can get location map on the mobile based on the Signal Strength. In the **MODIFICATION Part**, User selects the destination and the user gets the Map Image to reach the destination. During the mobility user could cross some other Bluetooth also, for example, if this project is implemented for a Hospital, User would select, Nero Department and will get the graph to reach that Department. During the path, user would be crossing Scan Department. Bluetooth installed in that scan department will send it's ID automatically to the user, even user can to fix appointment if he requires & can get the timings. This process will reduce waiting time spend on every Depart.

**ALGORITHM / METHODOLOGY:** RSS, Auto scanning Bluetooth

**DOMAIN:** Android, Mobile Computing, Embedded

**IEEE REFERENCE:** IEEE Paper on COMPSAC, 2013





# AADHITYAA INFOMEDIA SOLUTIONS

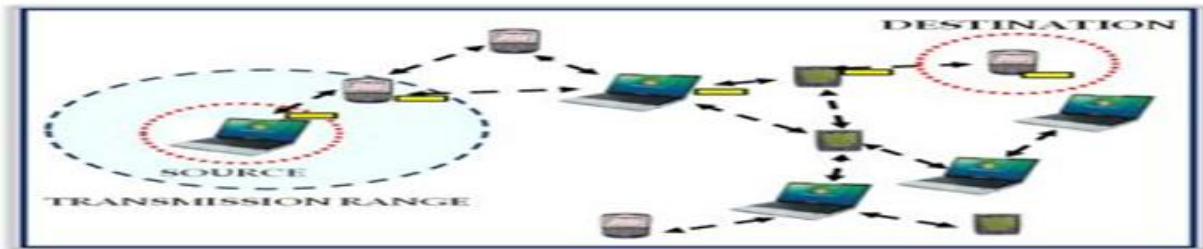
TRUST ME -  
CRISIL  
CERTIFIED

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



## NJA 4. ASSURED DATA TRANSMISSION USING FLOODING TIME, AND CAPACITY CALCULATION

### ARCHITECTURE DIAGRAM




**DATA IS TRANSMITTED THROUGH 1. FLOODING TIME,  
2. BROADCASTING SPEED, 3. NETWORK CAPACITY, 4. NODE MOBILTY  
WITH CAPACITY CALCULATION**

**DESCRIPTION:** In the **EXISTING SYSTEM**, due the fewer co-operations between the nodes and high Computation overhead will cause more problems in the Mobile Ad Hoc Networks. The data failure will happen during data transmission between the nodes. In the **PROPOSED SYSTEM**, we are implementing the three mechanisms namely, Flooding Time, Broadcasting Speed, Network Capacity and Node Mobility. The major objective is to identify the best Route to transfer the Data with maximum reliability. Flooding Time is used to identify the every nodes ID, route to transmit the data and Next Hops information. In the **MODIFICATION** Process, We are calculating the capacity of the available paths and to choose the best path for the data transmission between the mobile nodes.

**ALGORITHM / METHODOLOGY:** Flooding Time, Network Capacity

**DOMAIN:** MANET

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



## NJA 5 (DN 10012). 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

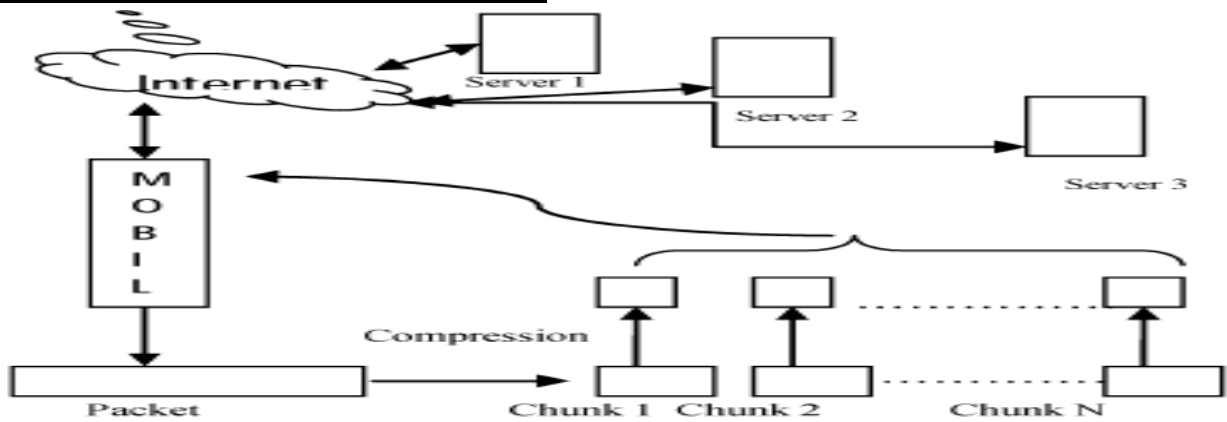
TRUST ME -  
CRISIL  
CERTIFIED

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



## NJA 6. INTEGRATION OF ANDROID & CLOUD COMPUTING IMPLEMENTATION OF REMOTE DATA STORAGE WITH CHUNKING OF DATA & COMPRESSION

### ARCHITECTURE DIAGRAM



**DESCRIPTION:** In the **EXISTING SYSTEM**, Mobile Storage Data is not transferable when you do carry USB card. There is no external data storage for Mobile. In the **PROPOSED SYSTEM**, Mobile data is Splitted into Smaller parts and stored into several Servers. This Process is called as Chunking. This Process ensures security. When ever the data is requested to the main server, all the data is rejoined and sent back to the requested User. Data is Compressed and retrieved. In the **MODIFICATION**, We are implementing Real-time Cloud Server then normal Server. We are using Drop box Cloud Server for effective data Storage and Retrieval. During Data retrieval automatic Key is generated which is used to verify the user.

**ALGORITHM / METHODOLOGY:** Random Key Generation, RLE

**DOMAIN:** Android, Mobile Computing

**IEEE REFERENCE:** IEEE Paper on WOCN, 2013



ISO / IEC 20000 CERTIFIED



BHARTIYA UDYOG  
RATAN - AWARDED



BITS PILANI  
PRACTICE SCHOOL



ISO 9001 : 2008 CERTIFIED



# AADHITYAA INFOMEDIA SOLUTIONS

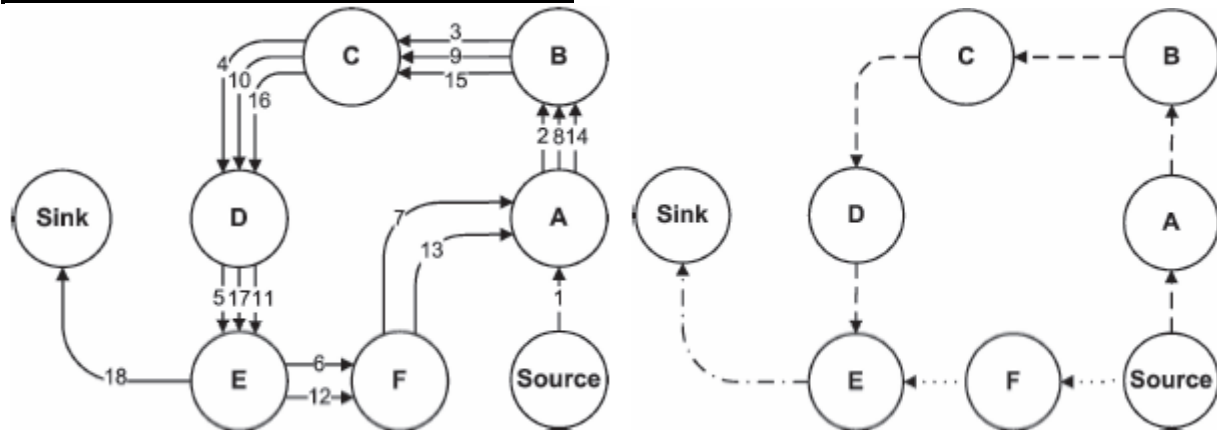
TRUST ME -  
CRISIL  
CERTIFIED

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



## NJA 7 (DN 10015). 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, Android, 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

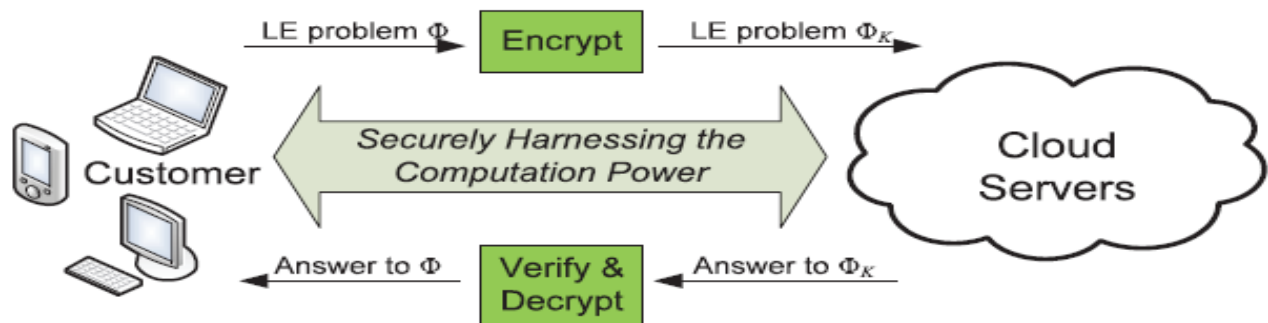
TRUST ME -  
CRISIL  
CERTIFIED

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



## NJA 8 (DN 10016). 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**

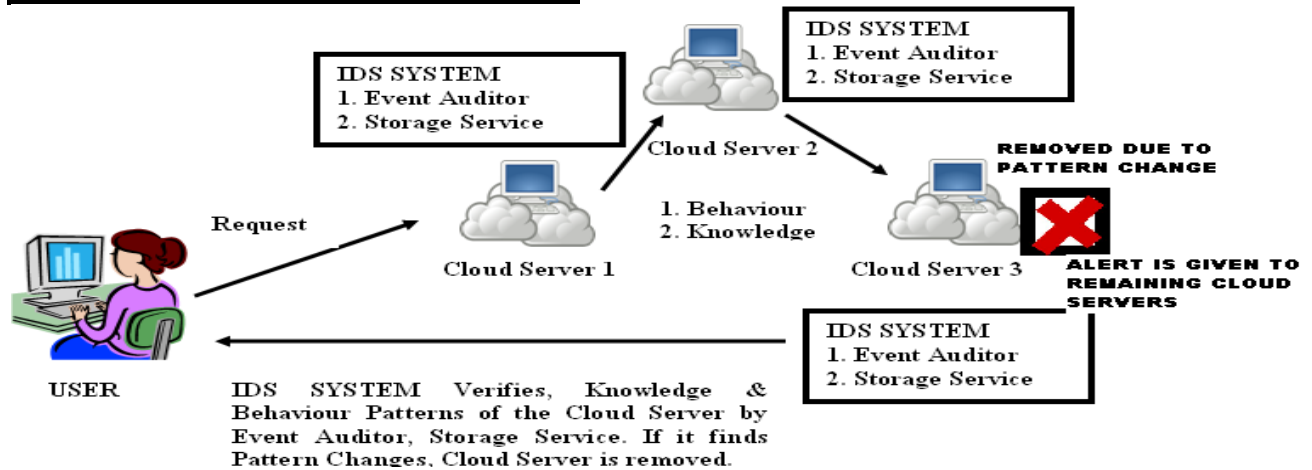
TRUST ME -  
CRISIL  
CERTIFIED

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



## NJA 9. ANDROID BASED SYSTEM TO DETECTION, MONITORING OF INTRUSION DETECTION SYSTEM (IDS)

### ARCHITECTURE DIAGRAM






**DESCRIPTION:** In the **EXISTING SYSTEM**, there is no proper security system is implemented in android platform even though lot of mobile user's presence. In the **PROPOSED MODEL**, IDS is implemented using two techniques namely analysis and detection. It is very helpful to detect the Attack. In the **MODIFICATION**, We implement Two Detection Methods.

1. Behavioral Approach is done by comparing the previous Behavior with the present Behavior.
2. Knowledge Approach is done by comparing the set of rules where Training Set is maintained and compared accordingly.

**ALGORITHM / METHODOLOGY: Behavior and Knowledge Algorithm**

**DOMAIN: Android, Mobile Computing, Cloud Computing**

**IEEE REFERENCE: IEEE Paper on BEIAC, 2013**

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



# AADHITYAA INFOMEDIA SOLUTIONS

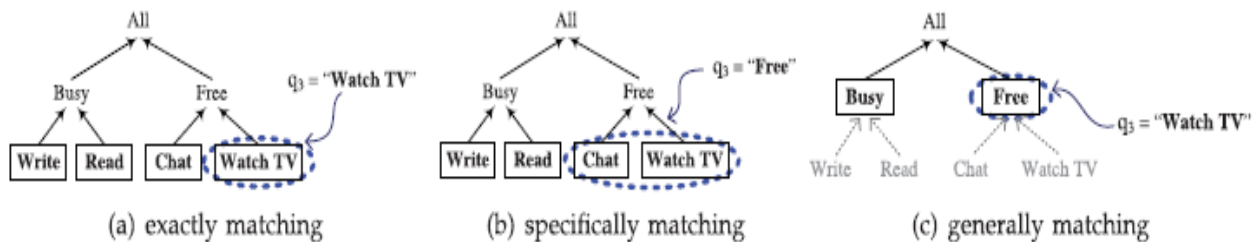
TRUST ME -  
CRISIL  
CERTIFIED

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



## NJA 10 (DN 10020). 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**

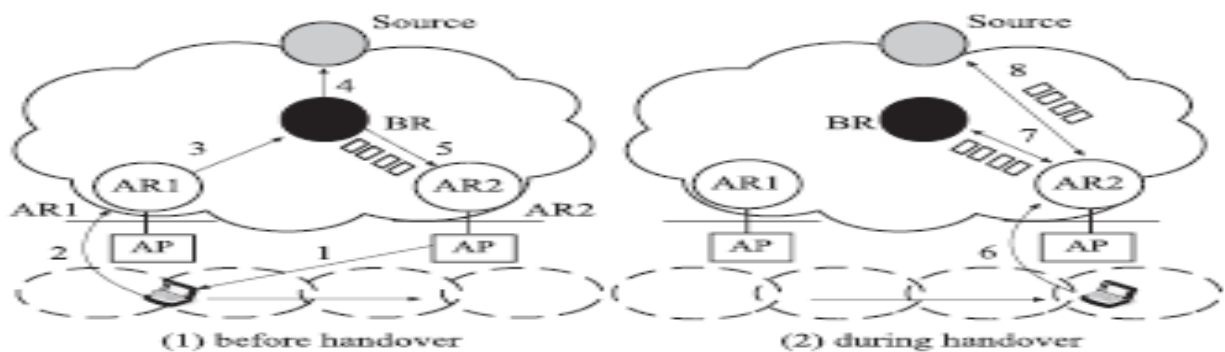
TRUST ME -  
CRISIL  
CERTIFIED

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



**NJA 11. IDENTIFICATION OF MOBILE NODES WITH  
MULTICAST ROUTING PROTOCOL WITH RELIABLE DATA  
DELIVERY**

**ARCHITECTURE DIAGRAM**



**DESCRIPTION:** In the **EXISTING SYSTEM**, methods still lack efficient multicast management and suffer from a long join latency, leading to a disappointing mobility performance. In the **PROPOSED SYSTEM**, Nodes are deployed or Positioned in a particular Access Router, these nodes can request a particular Service with its Node ID, Group ID and Service ID. Due to its Mobility, Nodes would have disconnected from that particular Access Router and would have joined with another Access Router. In the **MODIFICATION** Phase, if a User has requested a Service and due to its mobility requested data will be transmitted to the user without loss. Data is transmitted from Previous Router to the new router and finally to the user.

**ALGORITHM / METHODOLOGY: BRANCHING ROUTER BASED  
MULTICAST MANAGEMENT**

**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

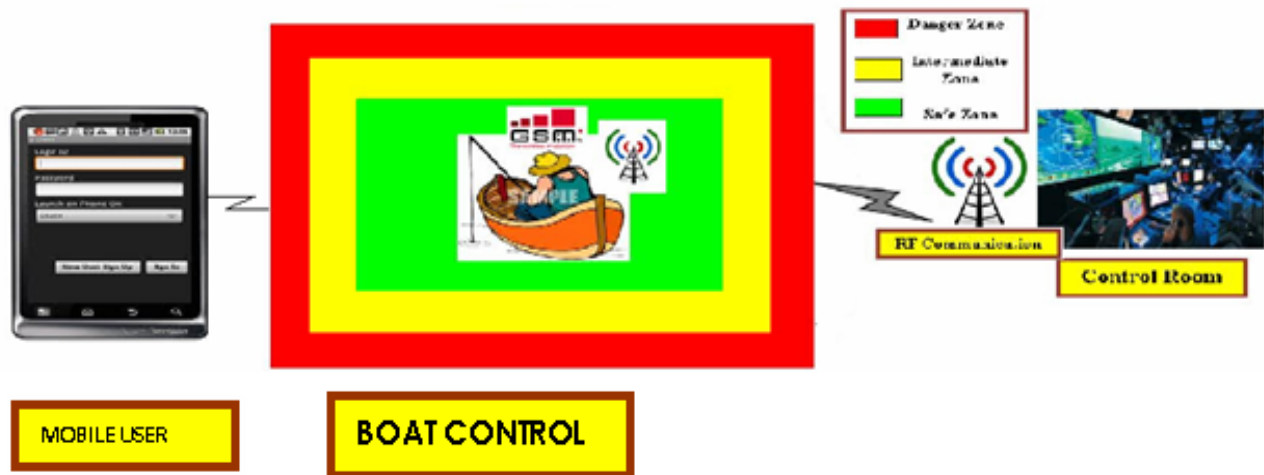
TRUST ME -  
CRISIL  
CERTIFIED

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



## NJA 12. ANDROID BASED BOAT CONTROL WITH AUTOMATIC SAFETY SYSTEM

### ARCHITECTURE DIAGRAM



**DESCRIPTION:** In the **EXISTING SYSTEM**, mobile devices are not connected with the external hardware components. In **PROPOSED MODEL**, hardware is constructed using embedded technology along with software application in android. Android is used to control the direction of the vehicle along with camera which can be fixed (if requires) for wireless video transmission. In **MODIFICATION**, same android application is developed for boat safety system. If boat is in the safe region, direction can be controlled using android. An alert is created and boat is stopped if it goes beyond the permitted region.

### ALGORITHM / METHODOLOGY:

**DOMAIN:** Android, Mobile Computing, Embedded

**IEEE REFERENCE:** IEEE Paper on MIRPO, 2013



ISO / IEC 20000 CERTIFIED



BHARTIYA UDYOG  
RATAN - AWARDED



BITS PILANI  
PRACTICE SCHOOL



ISO 9001 : 2008 CERTIFIED



# AADHITYAA INFOMEDIA SOLUTIONS

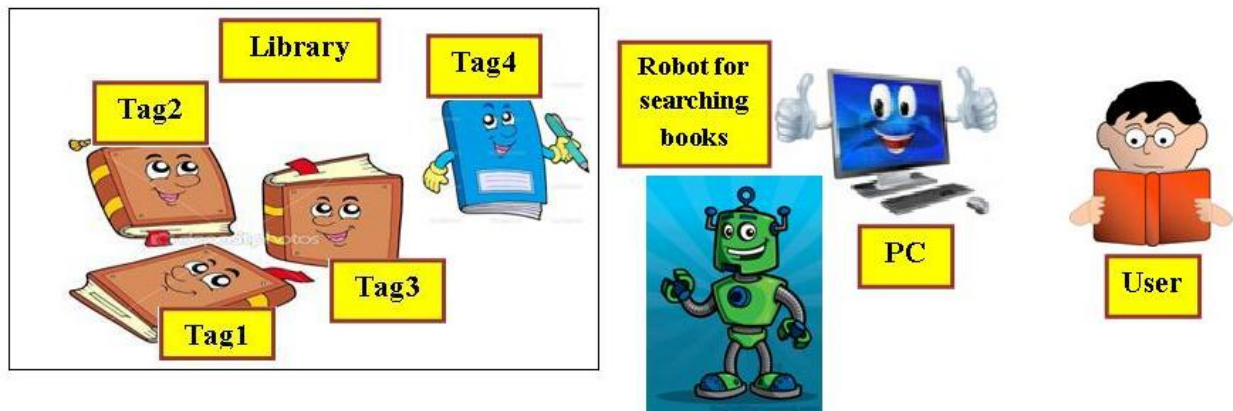
TRUST ME -  
CRISIL  
CERTIFIED

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



## NJA 13 (DN 10021). 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

 <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

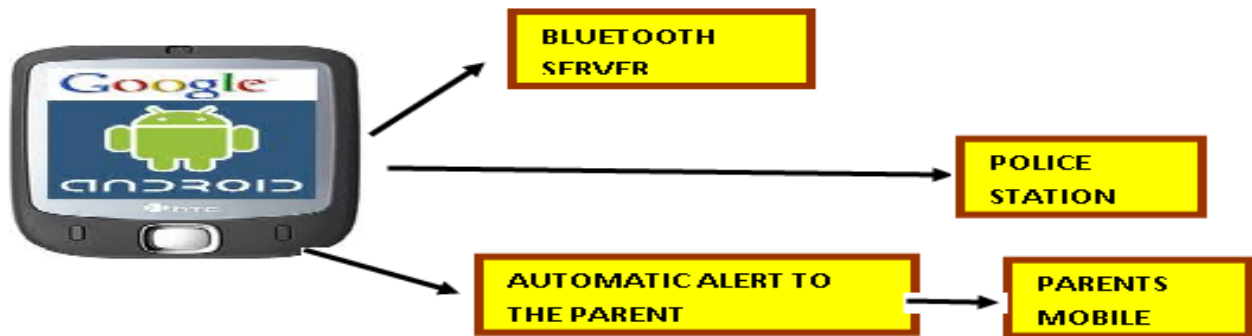
TRUST ME -  
CRISIL  
CERTIFIED

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



## NJA 14. LOCALIZATION & DETECTION OF EFFECTIVE TRACKING OF CHILDREN USING BLUETOOTH TECHNOLOGY

### ARCHITECTURE DIAGRAM




**DESCRIPTION:** In the **EXISTING SYSTEM**, children tracking system still a difficult task, as parents require server setup. In the **PROPOSED MODEL**, GPS, GSM voice recorder is provider to the children. Parents can send the request to the child’s embedded hardware and can track the location. But in our implementation / **MODIFICATION** we are using Bluetooth instead of GPS for identification of location change in Indoor navigation. If a child is move from expected region an automatic SMS alert is send to the parents mobile. An emergency situation also provided to the children, in case of emergency.

**ALGORITHM / METHODOLOGY:** Bluetooth Location Detection, SMS Service

**DOMAIN:** Android, Mobile Computing

**IEEE REFERENCE:** IEEE Paper on Communication & Signal Processing, 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

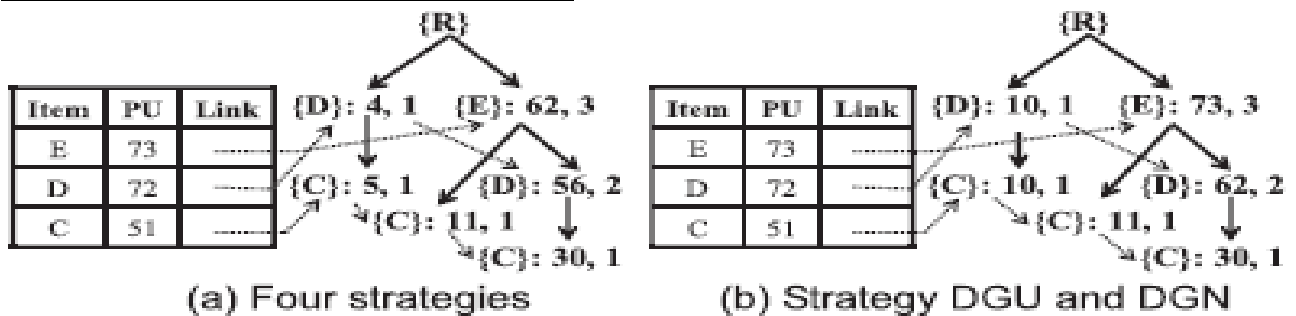
TRUST ME -  
CRISIL  
CERTIFIED

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



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

### ARCHITECTURE DIAGRAM

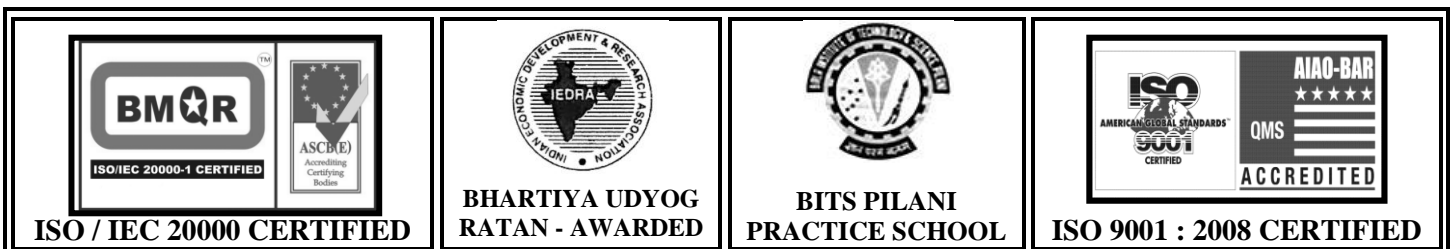


**DESCRIPTION:** In the **EXISTING SYSTEM**, In the framework of frequent item set mining, the importance of items to users is not considered. In the **PROPOSED SYSTEM**, User's interests of purchase of particular Products are monitored and Frequency Item set is extracted. Each node scan its local database 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**

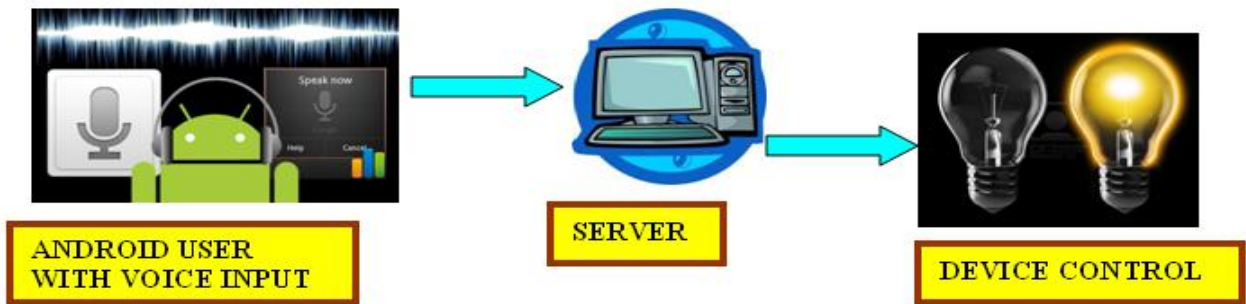
TRUST ME -  
CRISIL  
CERTIFIED

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



**NJA 16. VOICE DETECTION COMMAND CONTROL WITH  
FEEDBACK SYSTEM IN ANDROID ENVIRONMENT**

**ARCHITECTURE DIAGRAM**





**DESCRIPTION:** In the **EXISTING SYSTEM**, Indeed mobile has limited computational power as it is hand- held device, it is difficult to process voice commands. In the **PROPOSED MODEL**, user’s voice input is processed by the android mobile by converting voice to text and passes to embedded hardware for controlling. Once after it is controlled a reply alert is passed to the android user. In the **MODIFICATION** phase, as alert is provided to the user if power consumption crossing the permitted limit.

**ALGORITHM / METHODOLOGY:** Voice Detection, GPRS

**DOMAIN:** Android, Mobile Computing, Embedded

**IEEE REFERENCE:** IEEE Paper on ICCE, 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

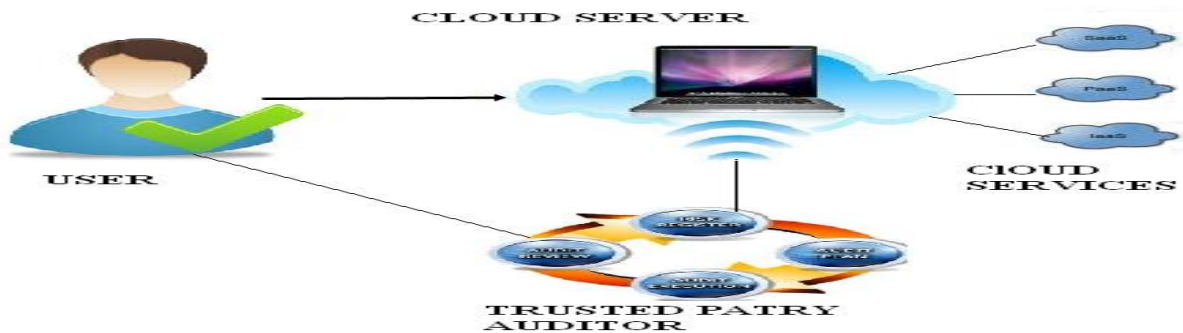
TRUST ME -  
CRISIL  
CERTIFIED

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



## NJA 17 (DN 10024). 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





# AADHITYAA INFOMEDIA SOLUTIONS

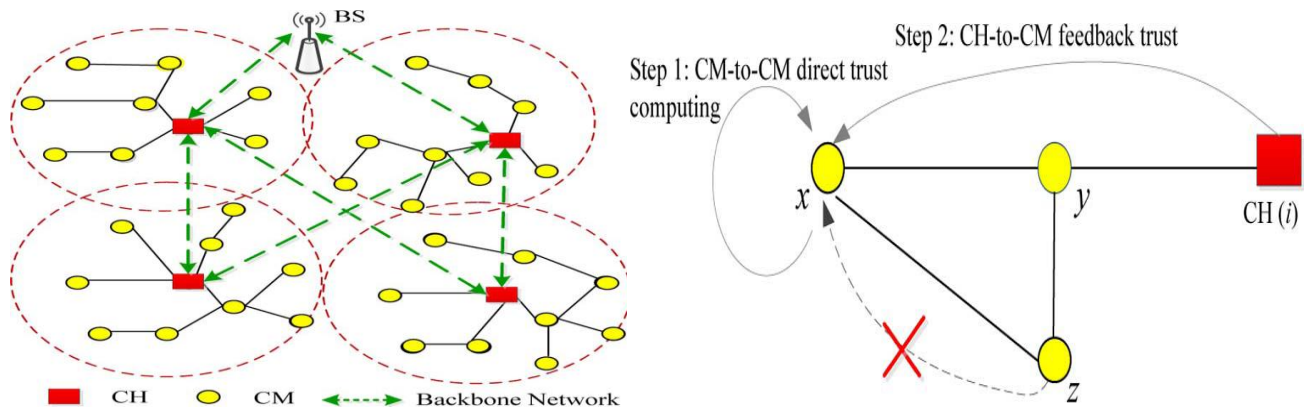
TRUST ME - CRISIL CERTIFIED

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



## NJA 18. DESIGN OF DEPENDABLE, TRUSTWORTHINESS OF DATA COMMUNICATION IN WSN

### ARCHITECTURE DIAGRAM







**DESCRIPTION:** In the **EXISTING SYSTEM**, In the wireless Sensor Networks are incapable of satisfying the resource efficiency and trust system because of the high overhead and low dependability. In the **PROPOSED MODEL**, Light Weight and Dependable Trust System (LDTS) is used which employees the Clustering Algorithm. The nodes are registered in every network and the Cluster Head is identified based on the Number of connections. We use feedback model to identify the best and most dependable route to reach the destination. The members are CM and their Heads are CH. Base Station acts as an Intermediate Node to Monitor the Data Transaction. BS will ask to give Feedback about their Neighbors in order to identify Trustworthiness. **MODIFICATION** that we propose is Packets are encrypted at the source.

**ALGORITHM / METHODOLOGY:** Clustering Algorithm, RSA

**DOMAIN:** Mobile Computing

**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

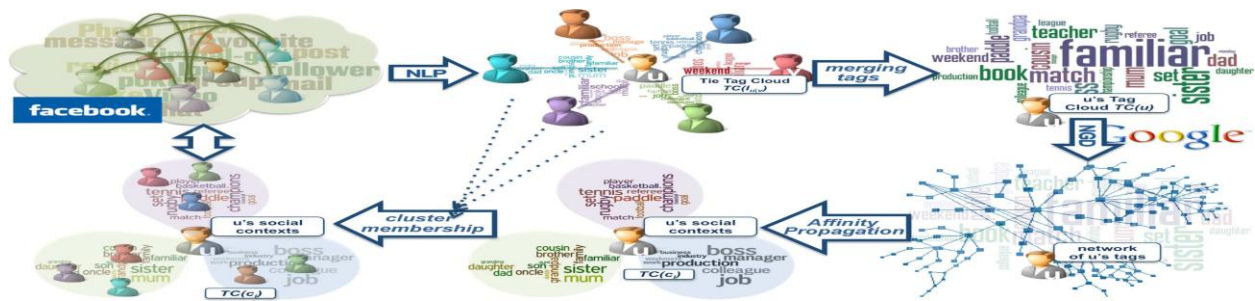
TRUST ME -  
CRISIL  
CERTIFIED

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



## NJA 19 (DN 10026). 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**

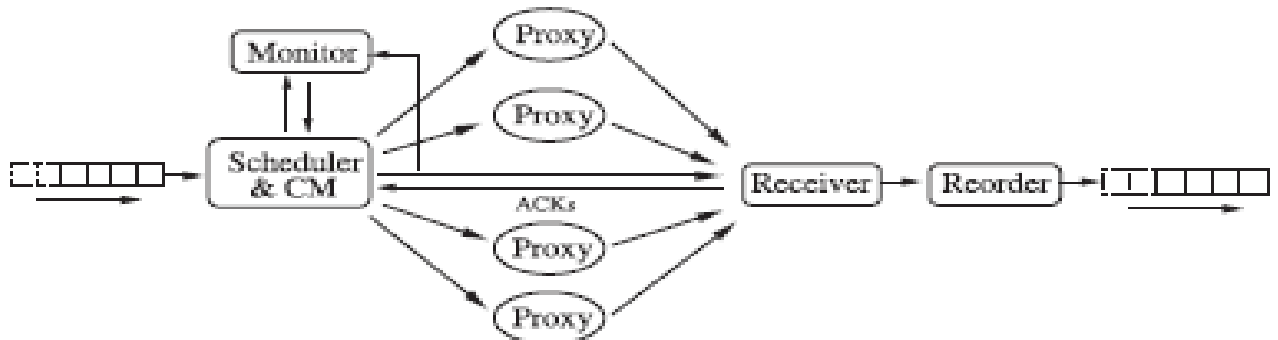
TRUST ME -  
CRISIL  
CERTIFIED

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



**NJA 20 (DN 10031). 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><b>ISO / IEC 20000 CERTIFIED</b></p>	 <p><b>BHARTIYA UDYOG RATAN - AWARDED</b></p>	 <p><b>BITS PILANI PRACTICE SCHOOL</b></p>	 <p><b>ISO 9001 : 2008 CERTIFIED</b></p>
---	--	--	---



# AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -  
CRISIL  
CERTIFIED

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



## NJA 21. BLUE GOAT: NEW APPROACH OF BLUE TOOTH BASED MISSED OBJECT TRACKING & DETECTION SYSTEM

### ARCHITECTURE DIAGRAM







**DESCRIPTION:** In the **EXISTING SYSTEM**, only Manual Students Attendance tracking is maintained, as for as Missed object tracking System, we will manually Search or make Police Complaint. In the **PROPOSED SYSTEM**, this paper deals about Students Attendance system, where Android Place with Bluetooth of the students is used to ping with the Staff mobile Phone. Once communication is establishes Attendance is marked. In the **MODIFICATION**, we are implementing the same concept but for different Application, Tracking the missed Object. Every Costlier Object that we are using is plugged with Bluetooth Device and a Buzzer. If user missed that object, he can send the Bluetooth pairing request from his Android Phone to that Object. If that missed object is present in that room / within its range, then automatically paring request is accepted & immediately buzzer alarms, so that user can easily identify the missed object.

**ALGORITHM / METHODOLOGY:** Source Routing Algorithm

**DOMAIN:** Mobile Computing, Android, Embedded

**IEEE REFERENCE:** IEEE Paper On ACCCCS, 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

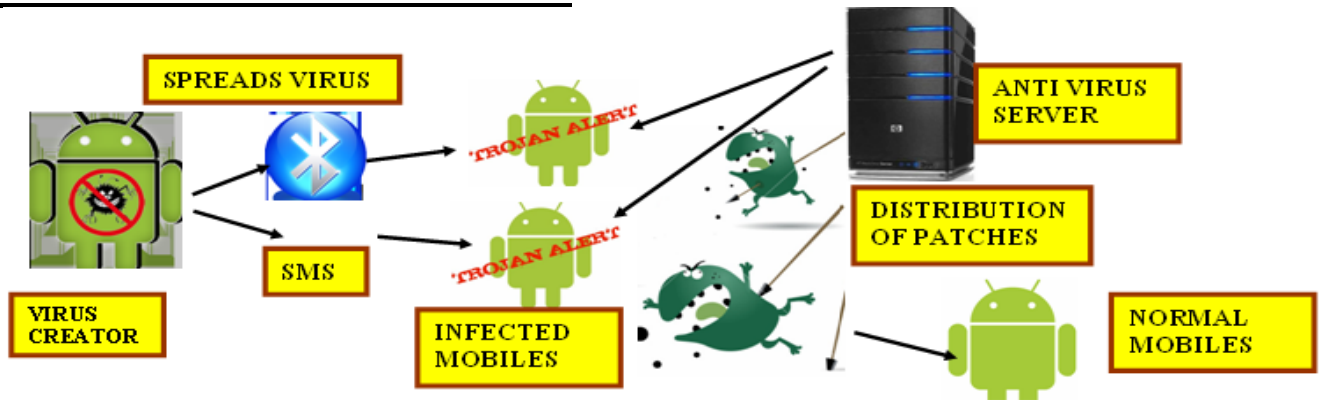
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6001. MOVID: MODELING AND AUTOMATIC DETECTION OF VIRUS IN MOBILE & SAAS – CLOUD BASED ANTI VIRUS SUPPORT WITH PATCHES DISTRIBUTION

### ARCHITECTURE DIAGRAM




**DESCRIPTION:** In the **EXISTING SYSTEM**, Viruses and malwares can spread from computer networks into mobile networks with the rapid growth of smart cellphone users. In a mobile network, viruses and malwares can cause privacy data leakage, extra charges, and remote listening. In the **PROPOSED MODEL**, we propose a two-layer network Process for Real time Model virus propagation through both Bluetooth and SMS. We Model a Virus and sent as SMS as well as Virus Data via Bluetooth to the other Users. As the users opens the SMS or the Data, Virus Spreads into their Mobile. Using Android Application Patches are distributed to the Affected Mobiles to clear the Virus in the Mobiles. The **MODIFICATION** we propose is that Automatic Alert is sent to the Server when Virus is affected in the Mobile, so that Patches is also automatically delivered to clear the Virus in the affected Mobiles. We have implemented Cloud computing for Software as a Service for Anti Virus Support and Patches Distribution

**ALGORITHM / METHODOLOGY:** Mobile virus propagation, Human Mobility

**DOMAIN:** Mobile Computing, Android, Cloud 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

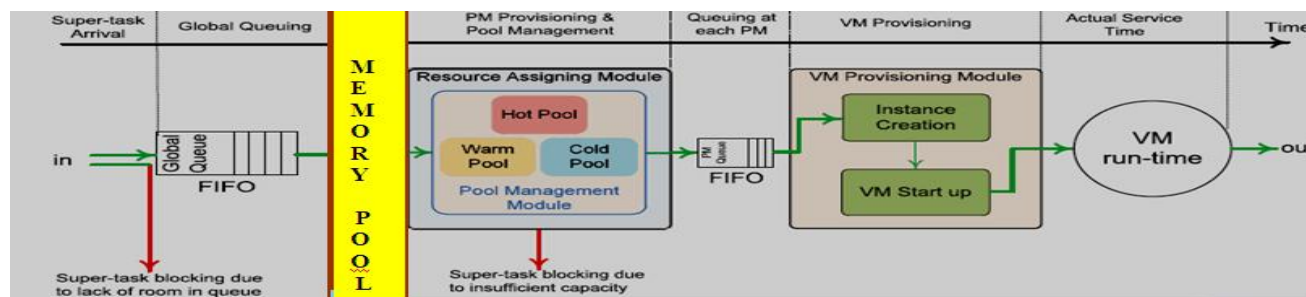
TRUST ME -  
CRISIL  
CERTIFIED

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



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

### ARCHITECTURE DIAGRAM







**DESCRIPTION :** In the **EXISTING SYSTEM**, Service availability and response time are two important quality measures in cloud's users perspective. A monolithic model may suffer from intractability and poor scalability due to large number of parameters. 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 processed by the Request Assigning Module (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 (1<sup>ST</sup>) ISO 20000, SEI CMMI LEVEL 3  
COMPLIANCE & ISO 9001 : 2008 CERTIFIED  
SOFTWARE DEVELOPMENT COMPANY)



## JA 6003 (DN 10002). DEVELOPMENT OF WIRELESS POWER TRANSMISSION FOR CHARGING PHYSICALLY CHALLENGED WHEEL CHAIR & 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

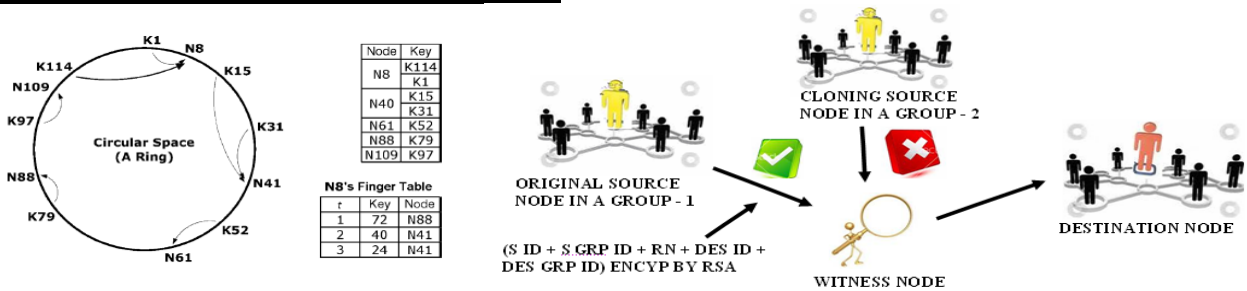
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6004 (DN 10003). 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





# AADHITYAA INFOMEDIA SOLUTIONS

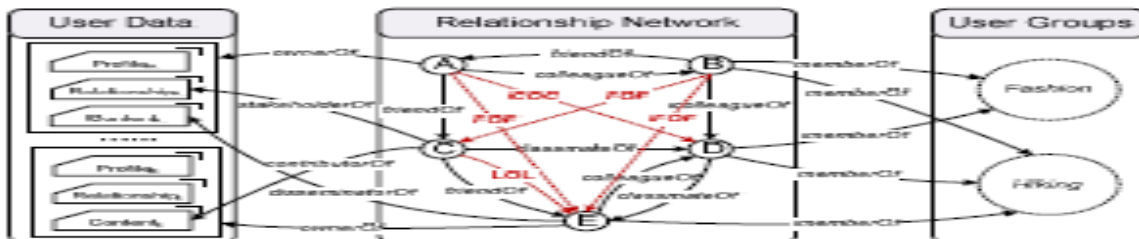
TRUST ME -  
CRISIL  
CERTIFIED

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



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

### 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**

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



# AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6006. CREDIT CARD FRAUD DETECTION: LOCATION BASED SECURITY SCHEME FOR SAFETY CARDS

### ARCHITECTURE DIAGRAM





**DESCRIPTION:** In the **EXISTING SYSTEM**, Credit Card Fraud is the most common occurrence. There is no authenticated step to control Credit Card Fraud in real time. In the **PROPOSED MODEL**, Location based Verification Scheme is implemented by comparing the User's Credit Card Location with the User's Mobile Location. This is very effective to identify the Real User. The **MODIFICATION** we propose is to generate an Encrypted Data to the Real User's Mobile Number along with the Decrypting Key as SMS only when both the Location of Credit Card and Mobile of the User is Matched. So process would definitely filter credit card fraud totally. We also provide a Emergency Key to the Authorized User to use only twice or Thrice to Withdraw Money during Emergency Situation for only for Rs. 2000 – 3000.

**ALGORITHM / METHODOLOGY:** Location Detection Algorithm

**DOMAIN:** Android, Security, Mobile Computing, Embedded

**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

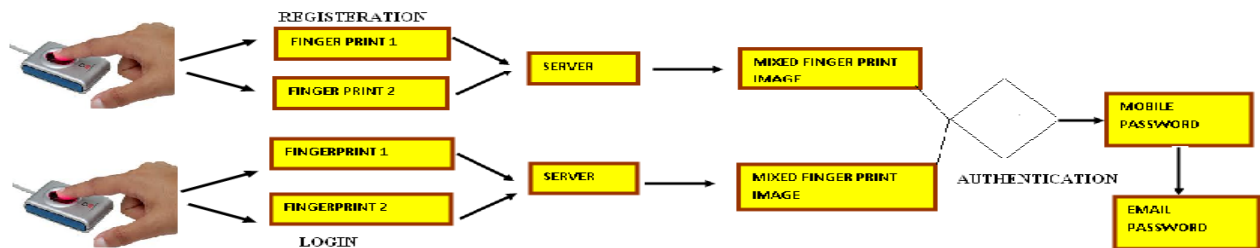
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6007. MIXED BIOMETRIC FINGERPRINT BASED USER AUTHENTICATION USING HASHING AND OTP GENERATION

### ARCHITECTURE DIAGRAM:






**DESCRIPTION:** In the **EXISTING SYSTEM** we are using only the textual passwords to authenticate user for accessing the applications. The textual passwords are easily hacked the hacker using online guessing attacks. So there is no big security implementation was introduced in the existing system. In the **PROPOSED SYSTEM**, we are using Mixed Fingerprint technique to provide more security for access the application. The user has to provide Two Different Finger prints while registration process and these finger prints are merged to form Mixed Fingerprint. Then During the login process, the user have to provide their both the finger prints and it will mixed again and compared with the original image. If the fingerprint is valid then the user is allowed to access the application. In the **MODIFICATION** process, Two Different One Time Passwords are generated and one is sent to the User's Mobile Number as SMS and another is sent as User's Email ID. Only after Authentication of Mixed Finger Print, Mobile OTP as SMS and E mail OTP User is allowed to access his/ her Banking Application.

**ALGORITHM / METHODOLOGY:** Secure Random Key Generation, Minutiae Fingerprint

**DOMAIN:** Image Processing, Biometrics, Security, Embedded

**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

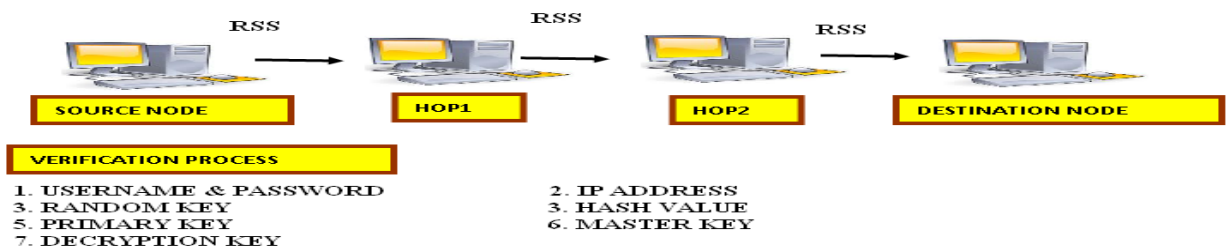
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6008 (DN 10009). 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

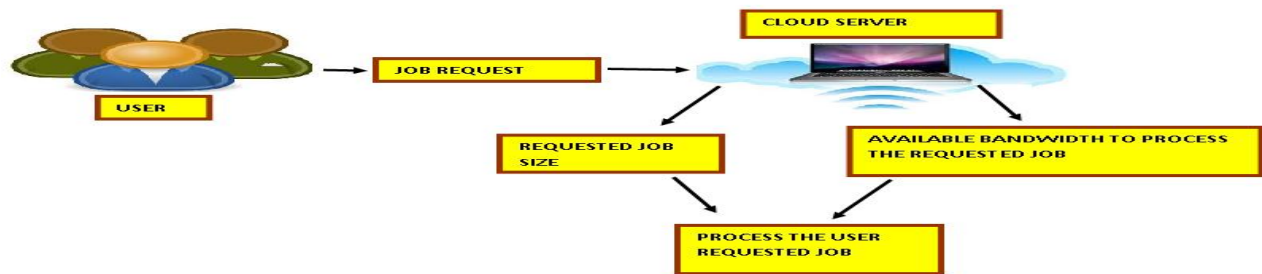
TRUST ME -  
CRISIL  
CERTIFIED

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



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

### 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



ISO / IEC 20000 CERTIFIED



BHARTIYA UDYOG  
RATAN - AWARDED



BITS PILANI  
PRACTICE SCHOOL



ISO 9001 : 2008 CERTIFIED



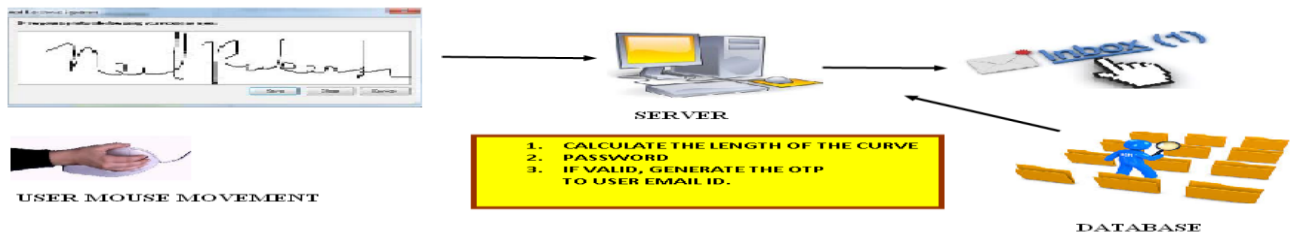
# AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6010 (DN10025). 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 (1<sup>ST</sup>) ISO 20000, SEI CMMI LEVEL 3  
COMPLIANCE & ISO 9001 : 2008 CERTIFIED  
SOFTWARE DEVELOPMENT COMPANY)



## JA 6011 (DN 10004).. 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

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



## JA 6012 (DN 10006). IMPLEMENTATION OF DATA SANITAZATION TECHNIQUE FOR EFFECTIVE FILTERING WITH ENCHANCED MEDICAL SUPPORT 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



ISO / IEC 20000 CERTIFIED



BHARTIYA UDYOG  
RATAN - AWARDED



BITS PILANI  
PRACTICE SCHOOL



ISO 9001 : 2008 CERTIFIED



# AADHITYAA INFOMEDIA SOLUTIONS

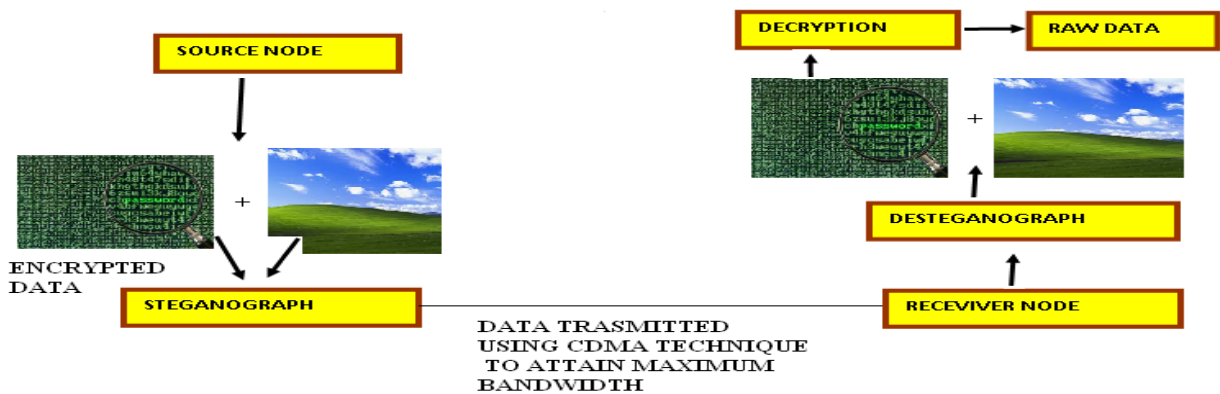
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6013 (DN 10035). 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

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



# AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6014 (DN 10007). 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

 <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

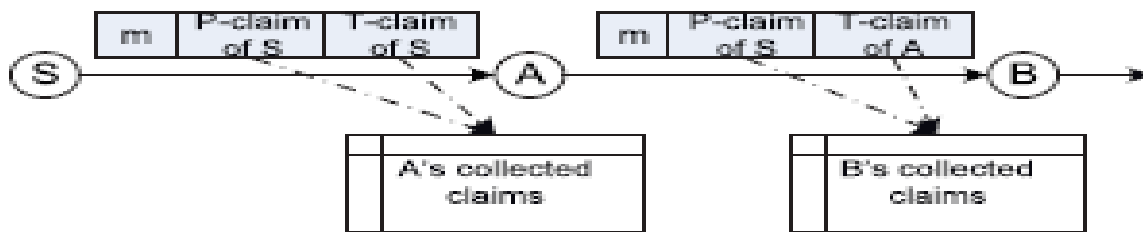
TRUST ME -  
CRISIL  
CERTIFIED

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



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

### ARCHITECTURE DIAGRAM

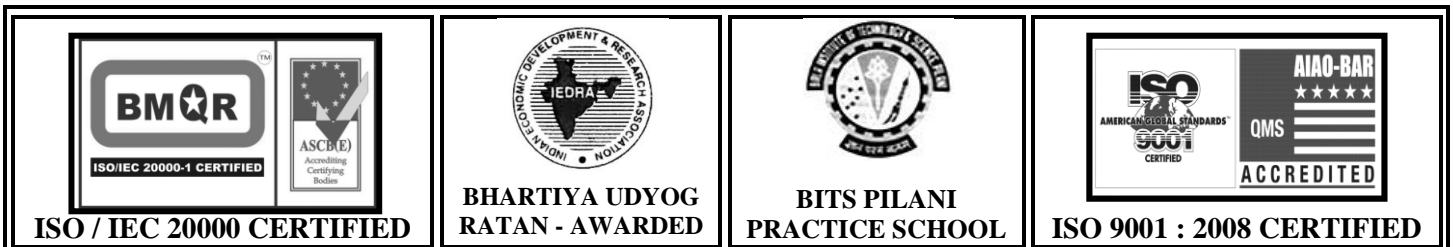


**DESCRIPTION :** In the **EXISTING SYSTEM**, DTNs consist of mobile nodes carried by human beings vehicles etc. when a node receives some packets, it stores in its Buffer and Forwards to another it contacts another. DTNs are vulnerable to flood attacks which would waste Buffer Resources of DTN. In the **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





# AADHITYAA INFOMEDIA SOLUTIONS

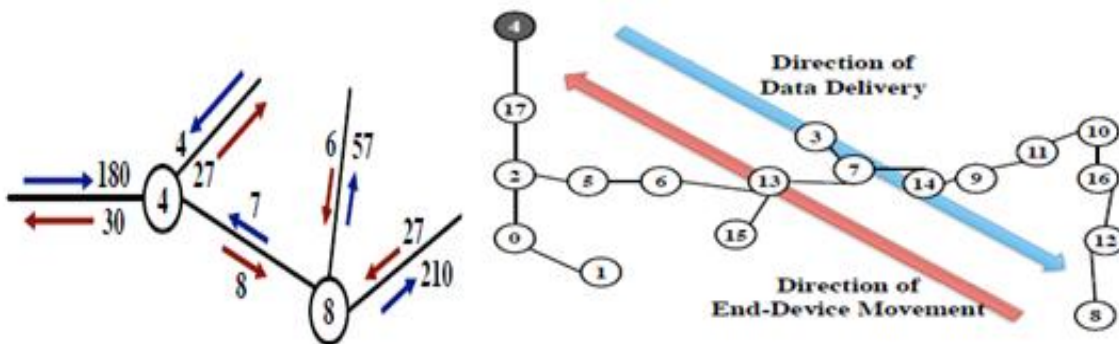
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6016. DESIGN OF ASSURED DATA DELIVERY USING INDEGREE AND CAPACITY CALCULATION IN WIRELESS LAN

### ARCHITECTURE DIAGRAM



**DESCRIPTION:** In the **EXISTING SYSTEM**, the ZigBee networks often uses a tree topology is to construct a WSN for data delivery applications. However, delivery failures occur constantly in ZigBee wireless applications due to node movements and also utilizes large amount of Resources. In the **PROPOSED SYSTEM**, the positions of the routers and design the tree topology so that most movements are directed towards the root of the tree. We first deploy the Nodes in a Network (**ZND**), then Calculate the Maximum In degree Node to find out Coordinator Node (**ZCD**), and finally Tree Construction in order to send the Data to the Destination (**ZTC**). In the **MODIFICATION PROCESS**, We are implementing the capacity calculation if In Degree node numbers are same in any two Nodes. We are not implementing Zigbee Network in this Project. We implement in Wireless Environment using Wireless LAN.

**ALGORITHM / METHODOLOGY:** ZND, ZTC, ZCD

**DOMAIN:** Networking

**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**

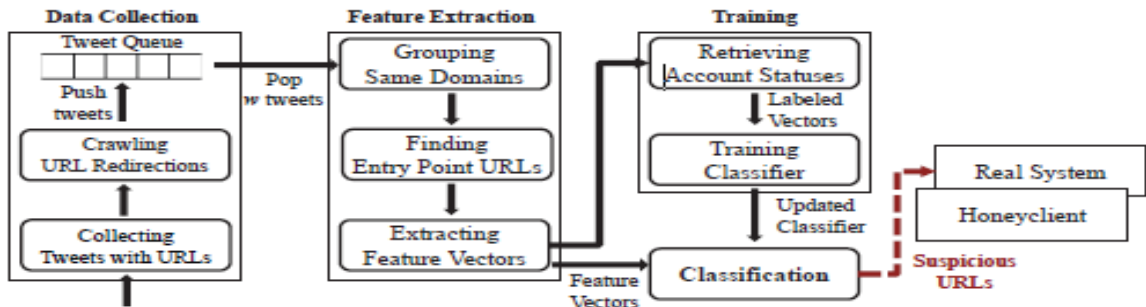
TRUST ME -  
CRISIL  
CERTIFIED

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



**JA 6017 (DN 10017). 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**

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



# AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6018 (DN 10036). 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

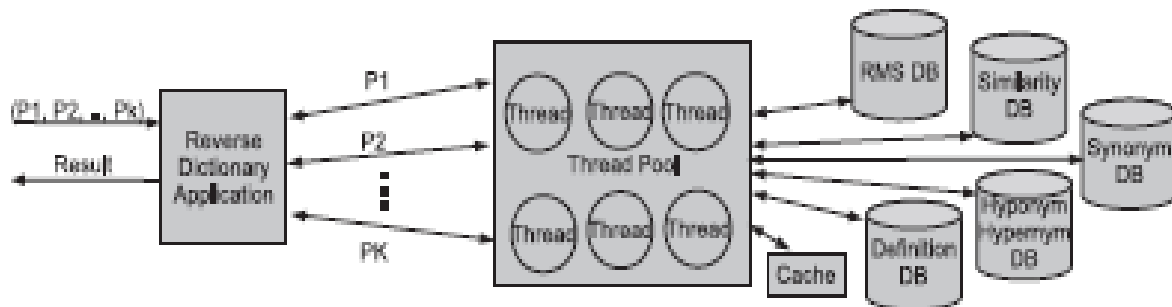
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6019 (DN 10018). 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



ISO / IEC 20000 CERTIFIED



BHARTIYA UDYOG  
RATAN - AWARDED



BITS PILANI  
PRACTICE SCHOOL



ISO 9001 : 2008 CERTIFIED





**AADHITYAA INFOMEDIA SOLUTIONS**

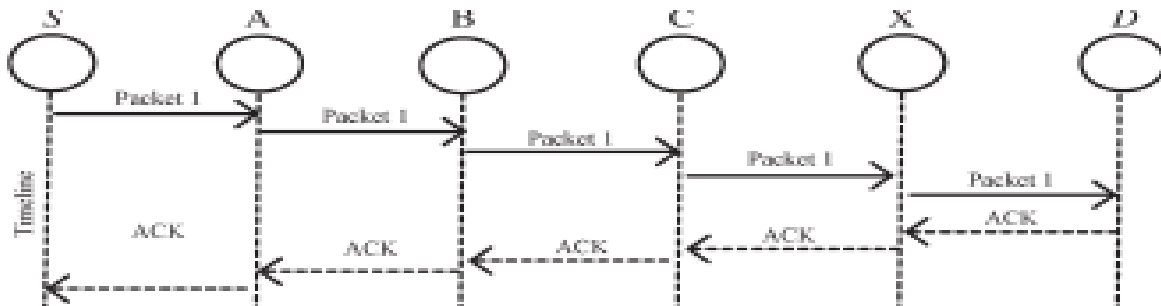
TRUST ME -  
CRISIL  
CERTIFIED

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



**JA 6020 (DN10019). 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

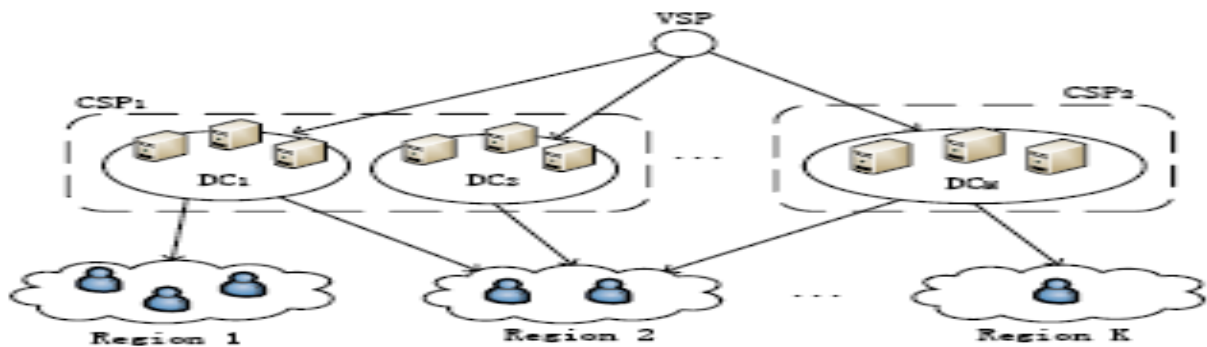
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6021. DESIGN OF EFFECTIVE BANDWIDTH/ RESOURCE MANAGEMENT SYSTEM FOR CLOUD ASSISTED VIDEO SHARING

### ARCHITECTURE DIAGRAM




**DESCRIPTION:** In the **EXISTING SYSTEM**, the high fluctuation of user demands in geographically distributed regions results in low resource utilizations of traditional CDN systems. In the **PROPOSED SYSTEM**, Multiple Cloud Server Data is Registered with Video Service Provider where all the videos are Stored. User will be requesting the video to their Region Head and the Region head will choose the Data Center for video Download. We apply 1. Nash Gaining Solution- for effective Resource Allocation based on User profile. 2. One Shot Atomization-Prediction of Maximum/ Best Bandwidth regional Servers. 3. Locality-Aware Peer- Analyzing and Allocation of Bandwidth based End-users' system provisioning In **MODIFICATION** process, Regional Servers will send the Request to the Best Data Center. Data Center will maintain its recent Videos in its Buffer, because same request can be processed from its center and not disturbing the Video Service Providers.

**ALGORITHM / METHODOLOGY:** Nash Bargaining Solution (NBS)

**DOMAIN:** Cloud Computing, Multi Media

**IEEE REFERENCE:** IEEE Transactions on Circuits and Systems for Video Technology, 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

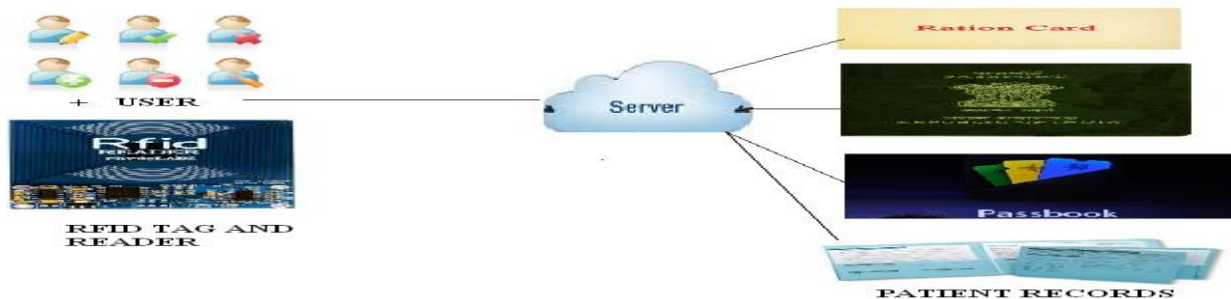
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6022. INTEGRATING WSN WITH WEB SERVICES FOR PATIENTS RECORDS FOR MANAGEMENT SYSTEM

### ARCHITECTURE DIAGRAM:



**DESCRIPTION:** In the **EXISTING SYSTEM** there is no big implementation for the Patient Health Record Management System. In the **PROPOSED SYSTEM**, the RFID is provided to the every User and the Web Service for Patient management system is deployed. Unique Patient's Id is stored in the RFID tag, for easy accessibility and patients are not required to bring the medical records every time to the Doctors. Once the Patient's RFID tag is shown to the reader, an automatic retrieval of patient records is achieved via web service Systems. In the **MODIFICATION PHASE** the Same RFID tag is utilized as the authentication tag for personal identification (Athor), Passport and Banking . Also we encrypt the User's information in the database for the security purpose.

### ALGORITHM / METHODOLOGY:

**DOMAIN:** Web Services

**IEEE REFERENCE:** IEEE Paper on Advanced 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

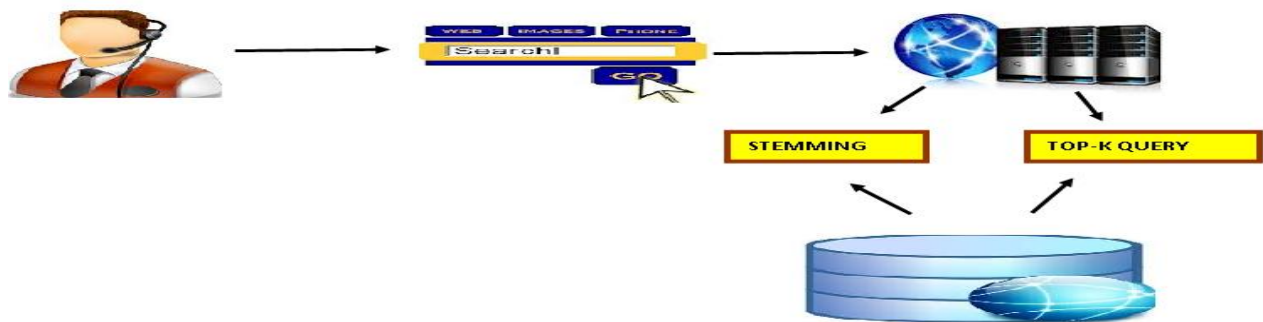
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6023 (DN 10027). 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

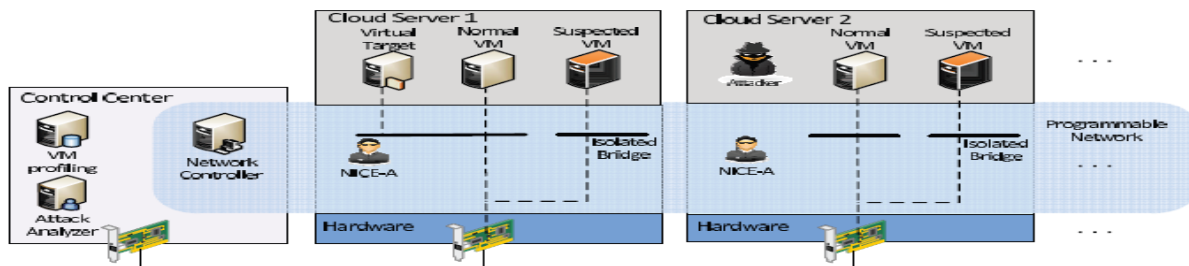
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6024. PROACTIVE DESIGN AND AVOIDANCE OF INTRUSION ATTACKS IN CLOUD DISTRIBUTED ENVIRONMENT

### ARCHITECTURE DIAGRAM






**DESCRIPTION:** Cloud security is one of most important issues that has attracted a lot of research and development effort in past few years. Particularly, attackers can explore vulnerabilities of a cloud system and compromise virtual machines to deploy further large-scale Distributed Denial-of-Service (DDoS). DDoS attacks usually involve early stage actions such as multistep exploitation, low-frequency vulnerability scanning, and compromising identified vulnerable virtual machines as zombies, and finally DDoS attacks through the compromised zombies. Within the cloud system, especially the Infrastructure-as-a-Service (IaaS) clouds, the detection of zombie exploration attacks is extremely difficult. This is because cloud users may install vulnerable applications on their virtual machines. To prevent vulnerable virtual machines from being compromised in the cloud, we propose multiphase distributed vulnerability detection, measurement, and countermeasure selection mechanism called NICE, which is built on attack graph-based analytical models and reconfigurable virtual network-based countermeasures.

**ALGORITHM / METHODOLOGY:** Alert Correlation Algorithm

**DOMAIN:** Network Security, Cloud Computing

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



## JA 6025 (DN 10013). 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**

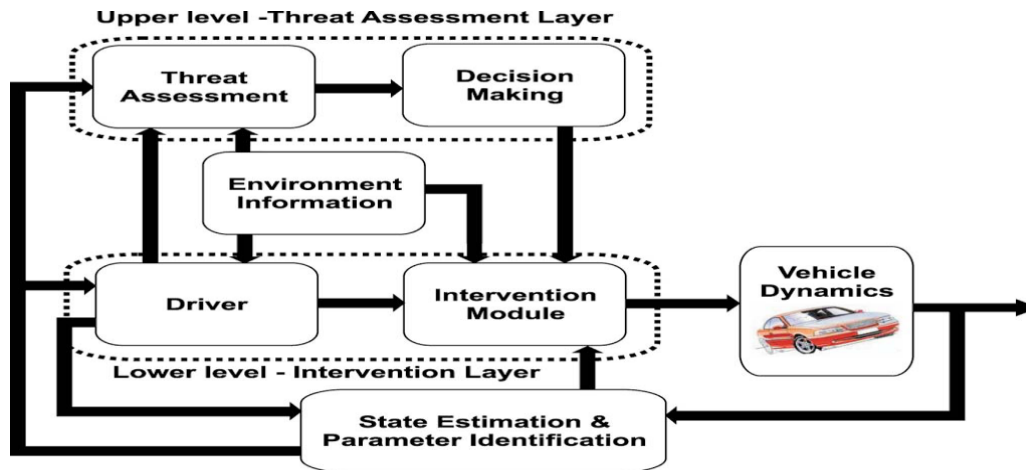
TRUST ME -  
CRISIL  
CERTIFIED

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



**JA 6026 (DN 10028). 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

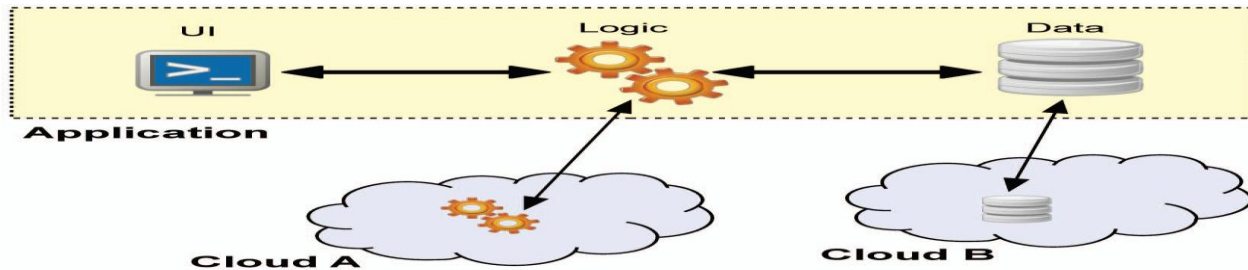
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6028. MULTI-CLOUD DEPLOYMENT WITH LOAD MANAGEMENT FOR SECURITY ANALYSIS

### ARCHITECTURE DIAGRAM



**DESCRIPTION:** In **EXISTING SYSTEM**, Although Cloud is vast developing technology, Security challenges are still a biggest obstacles when considering the adoption of cloud services. In the **PROPOSED SYSTEM**, we are implementing Multicloud Deployment System where one Cloud Server is utilized for Authorization/Verification and another as Resource Provide. Resource is deployed in one Cloud Server and Authority user, Authentication along with time of utility is monitored in another Cloud Server. The Major **MODIFICATION** in the Project is that we will be deploying the Resource in Two or More Cloud Servers. Authentication is processed by Another Cloud Server. Once Authentication is processes, then the CPU Load Monitoring is analyzed and best Cloud Server is identified for Resource Provision

**ALGORITHM / METHODOLOGY:** TurpinCoan

**DOMAIN:** Cloud Computing

**IEEE REFERENCE:** IEEE Transactions on Dependable and Secure 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 (1<sup>ST</sup>) ISO 20000, SEI CMMI LEVEL 3  
COMPLIANCE & ISO 9001 : 2008 CERTIFIED  
SOFTWARE DEVELOPMENT COMPANY)



## JA 6030. ATM: ANYTIME MEDICINE-ENCHANCED TELEMEDICINE WITH BIO-MEDICAL COMPUTATION IN CLOUD ENVIROMENT

### ARCHITECTURE DIAGRAM



**DESCRIPTION:** In the **EXISTING SYSTEM**, there is no remote method was implemented to monitor the patient. We need a Person to present nearby them and take care of them. In the **PROPOSED SYSTEM**, Telemonitoring of the patient is achieved. ATM (Any Time Medicine) machine is installed in the Rural Phase. Web camera is connected with the both Doctor and Patient End. Heartbeat, Temperature based Biomedical Hardware is connected to the Patient End along with medicine Dispatcher. Patient's biomedical values and Telemonitoring video conferencing is analyzed by the Doctor, then corresponding medicine is automatically issued to the patient from medicine dispatcher.

**ALGORITHM / METHODOLOGY:** RTP Protocol

**DOMAIN:** Embedded, Cloud Computing

**IEEE REFERENCE:** **IEEE Paper** on Information Communication and Embedded System, **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**

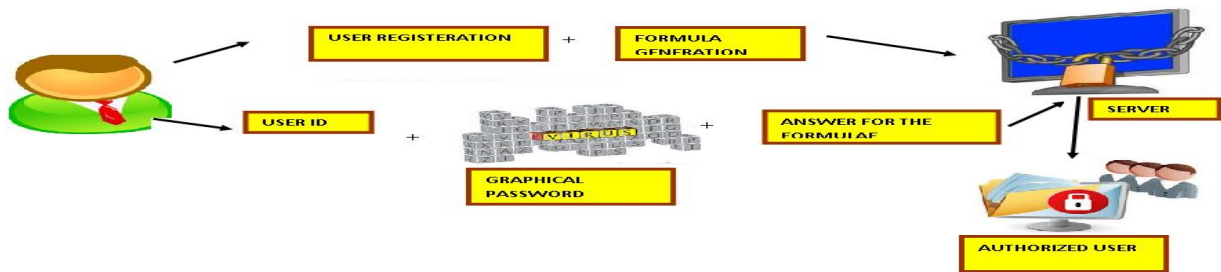
TRUST ME -  
CRISIL  
CERTIFIED

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



**JA 6031 (DN 10022). 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

 <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

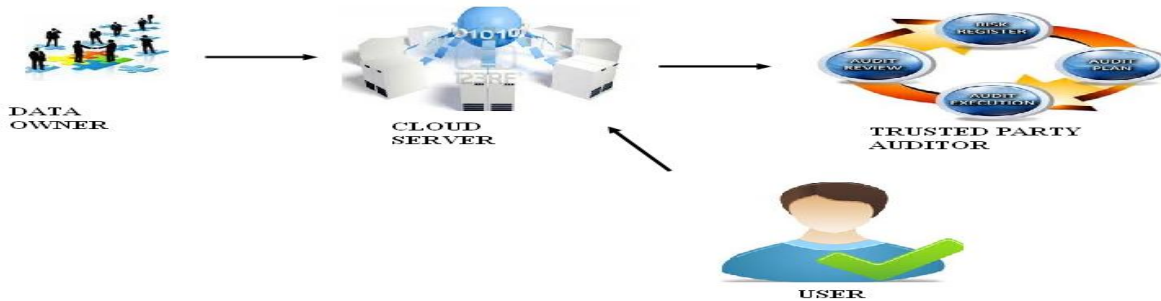
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6032 (DN 10038). 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 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
--	---	---	--



**AADHITYAA INFOMEDIA SOLUTIONS**

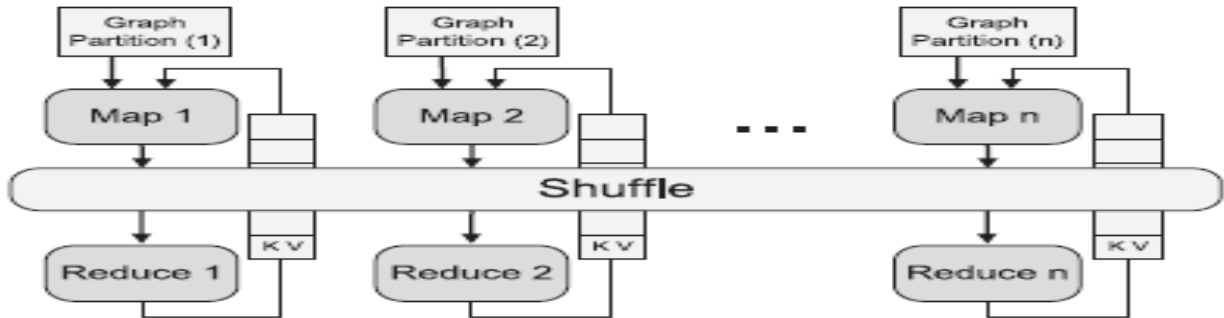
TRUST ME -  
CRISIL  
CERTIFIED

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



**JA 6033 (DN 10039). 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

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



**AADHITYAA INFOMEDIA SOLUTIONS**

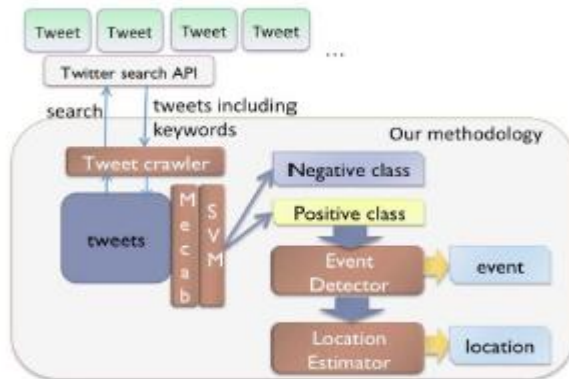
TRUST ME -  
CRISIL  
CERTIFIED

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



**JA 6034 (DN 10040). 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 (1<sup>ST</sup>) ISO 20000, SEI CMMI LEVEL 3  
COMPLIANCE & ISO 9001 : 2008 CERTIFIED  
SOFTWARE DEVELOPMENT COMPANY)



## JA 6035. LOCATION BASED USER TRACKING FOR AUTHORIZED DATA ACCESS

### ARCHITECTURE DIAGRAM



**DESCRIPTION:** In the **EXISTING SYSTEM**, user Location is usually tracked using GPS, but GPS cannot be used or the internal tracking. So there is no effective Location Tracking Mechanism. In the **PROPOSED MODEL**, A Privacy-Preserving Location proof Updating System (APPLAUS) in which colocated mobile devices mutually generate location proofs and send updates to a location proof server. Periodically changed pseudonyms are used by the mobile devices to protect source location privacy from each other, and from the untrusted location proof server. **MODIFICATION** that we Propose in this Project, is to Automatic Alert SMS to the Main Server about the particular User's Misbehavior, So that the Admin can take necessary action against the user if required.

**ALGORITHM / METHODOLOGY:** Location Proof Update Scheduling

**DOMAIN:** Android, Mobile Computing, Security

**IEEE REFERENCE:** IEEE TRANSACTIONS on Mobile computing, 2013

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



# AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -  
CRISIL  
CERTIFIED

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



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

### ARCHITECTURE DIAGRAM

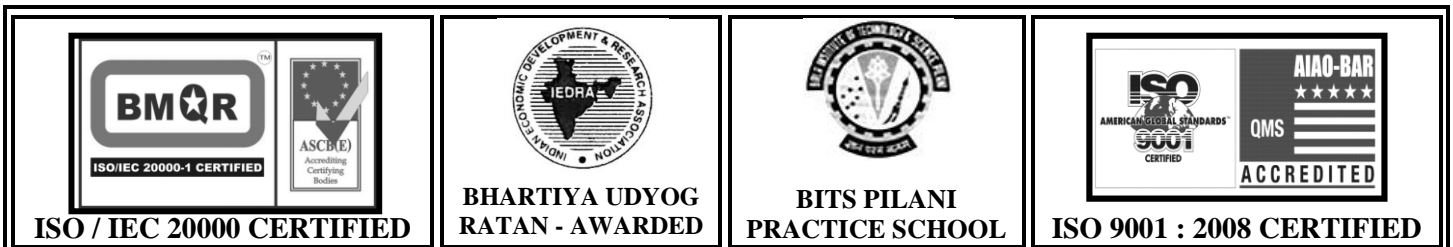


**DESCRIPTION:** In the **EXISTING SYSTEM**, Personal health record (PHR) is an emerging patient-centric in Cloud Computing Servers. However, there is no Security in keeping privacy concerns of the Patient & could be exposed to those third party servers and to unauthorized parties. In the **PROPOSED 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

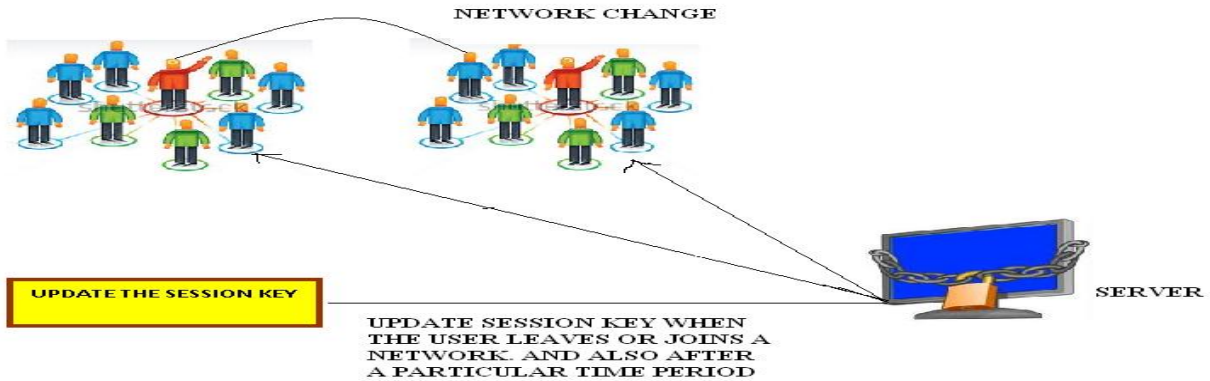
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6037 (DN 10041). 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

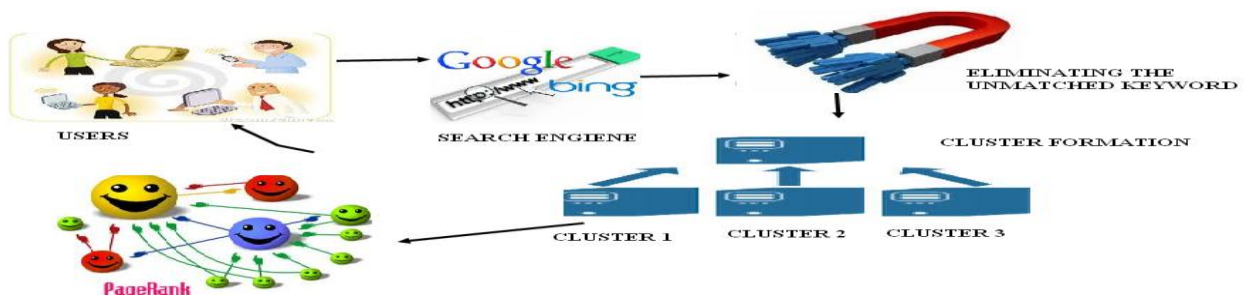
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6038 (DN 10033). 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

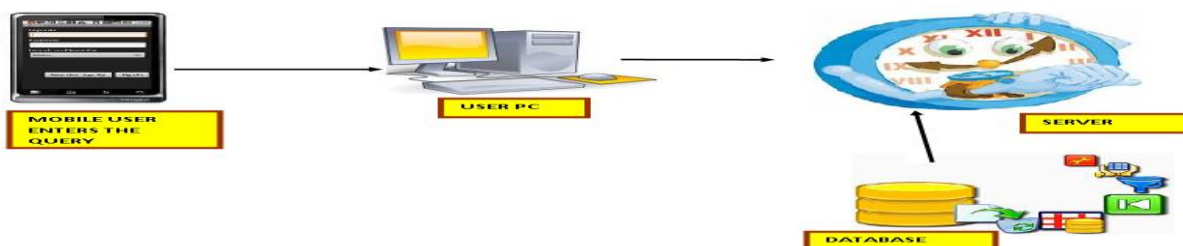
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6039. ANDROID ONTOLOGY BASED COMPRABLE SEARCH ENGINE WITH DUPLICATES REMOVAL USING UDD

### ARCHITECTURE DIAGRAM



**DESCRIPTION :** In the **EXISTING SYSTEM**, A major problem in mobile search is that the interactions between the users and search engines are limited by the small form factors of the mobile devices. As a result, mobile users tend to submit shorter, hence, more ambiguous queries compared to their web search counterparts. In the **PROPOSED MODEL**, users search's on the when for query, either Area specified (or) user's location, server retrieves all the information to the user's PC where ontology is applied. User PC displays all the relevant keywords to the user's mobile, so that user selects the exact requirement. Ranking occurs and finally exactly mapped information is produced to the user's mobile. In the **MODIFICATION**, We apply UDD algorithm to eliminate the duplication of records which helps to minimize the number of URL listed to the user.

**ALGORITHM / METHODOLOGY:** Naive Bayes classifier, Ontology, UDD

**DOMAIN:** Mobile Computing, Android, 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

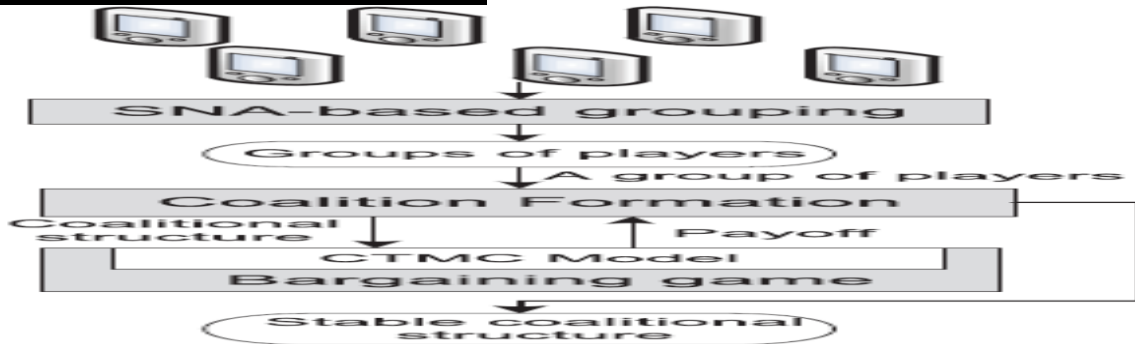
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6040 (DN 10042). 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**

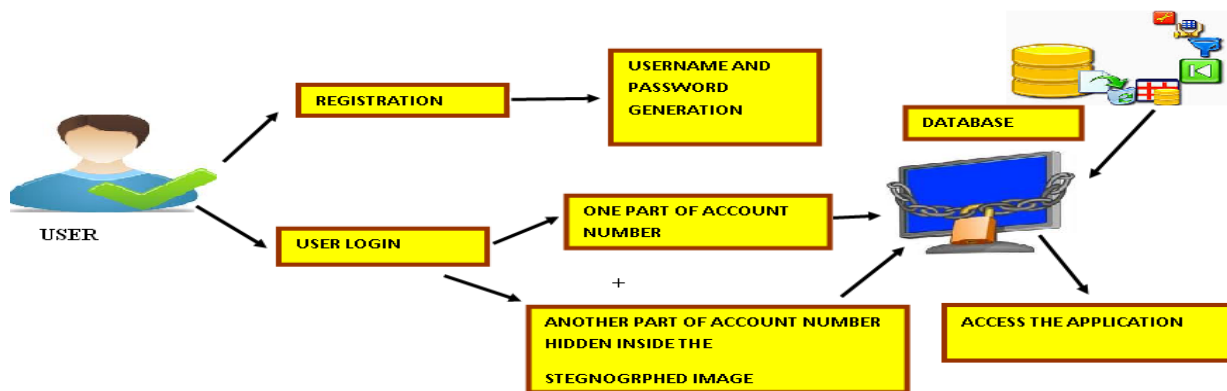
TRUST ME -  
CRISIL  
CERTIFIED

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



**JA 6041 (DN 10029). 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**

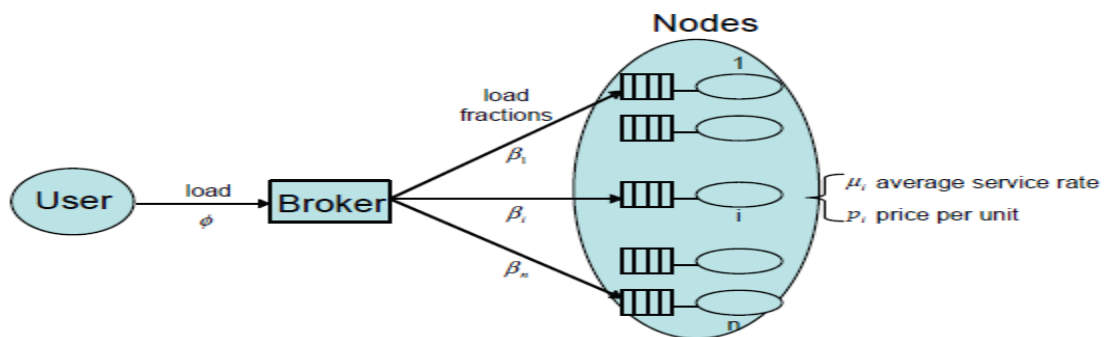
TRUST ME -  
CRISIL  
CERTIFIED

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



**JA 6042. ON THE DESIGN OF MUTUALLY AWARE OPTIMAL  
PRICING AND LOAD BALANCING STRATEGIES FOR GRID  
COMPUTING SYSTEMS**

**ARCHITECTURE DIAGRAM**






**DESCRIPTION:** Managing resources and cleverly pricing them on computing systems is a challenging task. Resource sharing demands careful load balancing and often strives to achieve a win-win situation between resource providers and users. Toward this goal, we consider a joint treatment of load balancing and pricing. We do not assume static pricing to determine load balancing, or vice versa. Instead, we study the relationship between the price that a computing node is charged and the load and revenue that it receives. We find that there exists an optimal price which maximizes the revenue. We then consider a multiuser environment and explore how the load from a user can be balanced on processors with existing loads. Finally, we derive an optimal price that maximizes the revenue in the multi-user environment.

**ALGORITHM / METHODOLOGY:** Pricing

**DOMAIN:** Grid Computing

**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

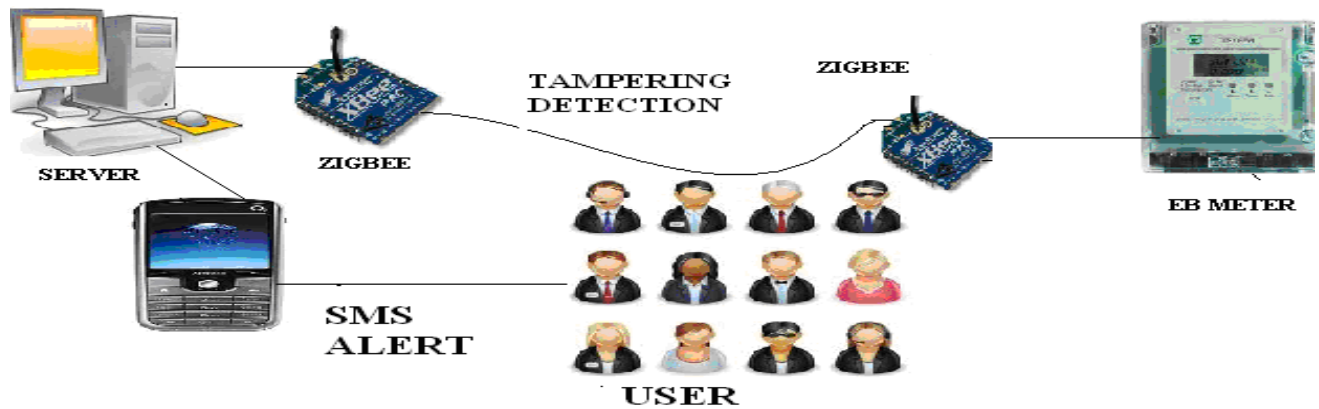
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6044 (DN 10043). 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 (1<sup>ST</sup>) ISO 20000, SEI CMMI LEVEL 3  
COMPLIANCE & ISO 9001 : 2008 CERTIFIED  
SOFTWARE DEVELOPMENT COMPANY)



## JA 6045. INTEGRATED IMPLEMENTATION OF AUTOMATED CONTROL MECHANISM FOR MUSIC PLAYER, SYSTEM AND FILE TRANSFER IN ANDROID ENVIRONMENT

### ARCHITECTURE DIAGRAM





**DESCRIPTION:** In the **EXISTING SYSTEM**, we are only able to control the volume of the players in the Short Distance using IR sensors and also control the system manually. There is no implementation was introduced. In the **PROPOSED SYSTEM**, we are developing an Android Application in order to control the volume of Earing Aid using Bluetooth. In the **MODIFICATION** we are developing an Android Application to control the music player using GPRS connectivity. We also can control the system Shutdown, Restore, Logout process from the remote place. We can also transfer a File from the Mobile to the Remote Serer and we can retrieve the File when it is required.

### ALGORITHM / METHODOLOGY:

**DOMAIN:** Android, Networking

**IEEE REFERENCE:** IEEE Paper on Consumer 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

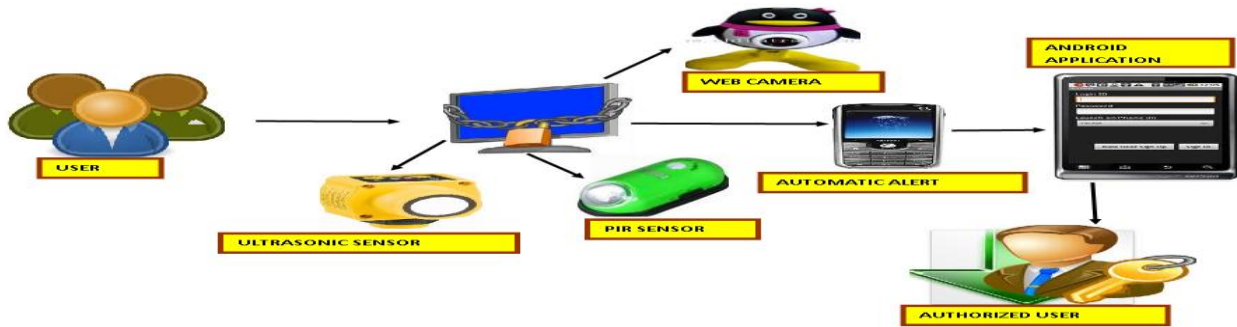
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6046. HUMAN SURVEILLANCE DETECTION USING ULTRASONIC & PIR WITH IMAGE BASED MOTION DETECTION USING NEURAL NETWORK IN ANDROID PALTFORM

### ARCHITECTURE DIAGRAM





**DESCRIPTION:** In the **EXISTING SYSTEM**, the Remote Video Surveillance System is carried using Live Video Transformation to TV. Admin has to see those Videos continuously. In the **PROPOSED SYSTEM**, we use two sensors namely Ultrasonic and PIR. Ultrasonic is used to detect the obstacle and PIR is used to detect the Human temperature presence in the particular area. If both Ultrasonic and PIR is detected, only then web camera is initialized to capture the images for the surveillance system. In the **MODIFICATION** part, an Android application is developed for the administrator to view the motion detected image from the Server. Also an automatic SMS alert is generated from the Server to the administrator if motion is detected. Administrator can view the images and take action accordingly.

### ALGORITHM / METHODOLOGY:

**DOMAIN:** Android, Mobile Computing, Security, Embedded.

**IEEE REFERENCE:** IEEE Paper on Embedded 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

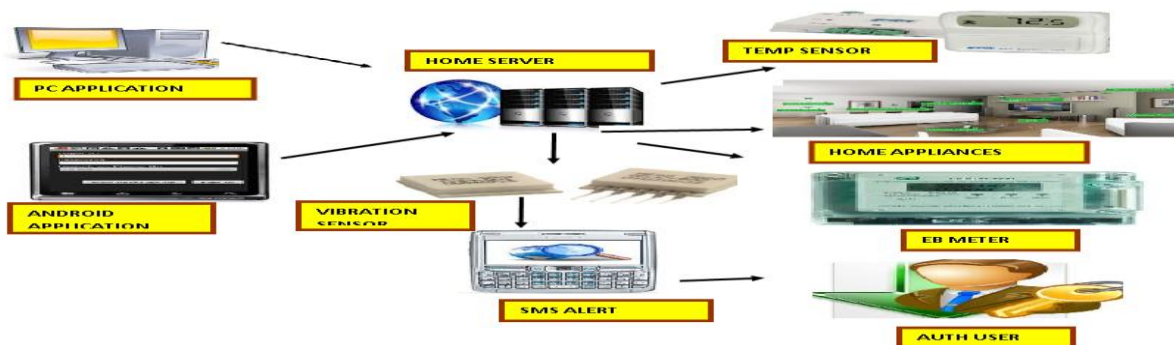
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6047. MULTI INPUT CONTROL MECHANISM OF HOME SECURITY SYSTEM USING ANDROID

### ARCHITECTURE DIAGRAM



**DESCRIPTION:** In the **EXISTING SYSTEM**, with the development of social economy more appliances has been present in the house and there is no automated system control mechanisms. In the **PROPOSED MODEL**, an Application is developed in both PC as well as in Android Smart Phones. The Sensors like Temperature, Humidity, and Gas is connected in the house environment along with the devices. User can control the electrical appliances via the PC or Mobile Phones from the Remote Place. Data Acquisition System is achieved by getting the relevant sensor values from the remote place. An EB Meter is also attached to calculate the Meter Readings. In the **MODIFICATION**, a vibration Sensor is connected to the House which detects the vibration in order to ensure the Home Security System. An automatic alert is generated to the administrator for both the Gas leakage and Vibration Detection.

### ALGORITHM / METHODOLOGY:

**DOMAIN:** Android, Mobile Computing, Security, Embedded.

**IEEE REFERENCE:** IEEE Paper on Intelligent Control and Information Processing, 2013



ISO / IEC 20000 CERTIFIED



BHARTIYA UDYOG  
RATAN - AWARDED



BITS PILANI  
PRACTICE SCHOOL



ISO 9001 : 2008 CERTIFIED



# AADHITYAA INFOMEDIA SOLUTIONS

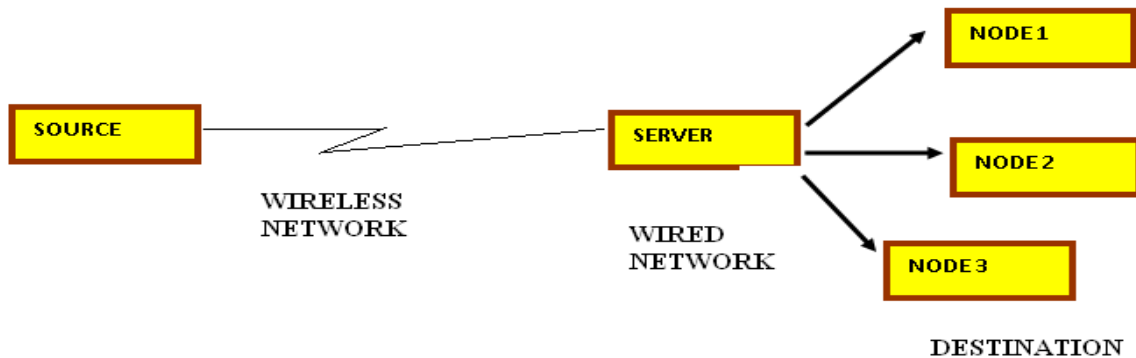
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6048 (DN 10044). REALITY IMPLEMENTATION OF HYBRID COMMUNICATION IN WIRED AND WIRELESS NETWORKS.

### ARCHITECTURE DIAGRAM




**DESCRIPTION:** In the **EXISTING SYSTEM**, the zigbee networks and UMTS networks are working separately. There is no implementation to merge the two networks and creating a new network for data processing. In the **PROPOSED SYSTEM**, we will combine the two networks and develop the hybrid network in which the data is transferred from source node (Wireless) to the destination node via the server which is connected through LAN. In the **MODIFICATION** Process, We are not implementing Zigbee Network in this Project. We implement in Wireless Environment using Wireless LAN.

**ALGORITHM/METHODOLOGY:** Ad hoc On Demand Distance Vector

**DOMAIN:** Networking

**IEEE REFERENCE:** IEEE Paper on Communications, 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

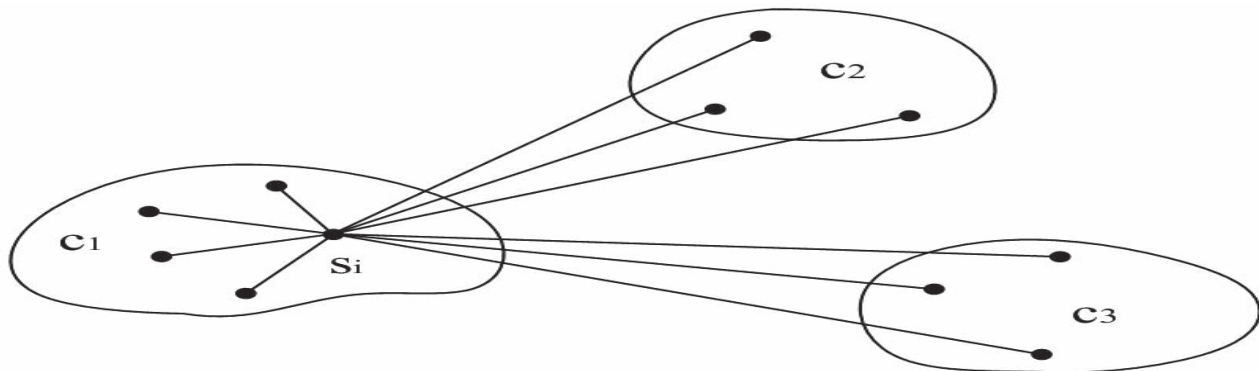
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6049 (DN 10030). 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 (1<sup>ST</sup>) ISO 20000, SEI CMMI LEVEL 3  
COMPLIANCE & ISO 9001 : 2008 CERTIFIED  
SOFTWARE DEVELOPMENT COMPANY)**



**JA 6050. A DECENTRALIZED SELF-ADAPTATION  
MECHANISM FOR SERVICE-BASED APPLICATIONS IN THE  
CLOUD**

**ARCHITECTURE DIAGRAM**



**DESCRIPTION:** Cloud computing, with its promise of (almost) unlimited computation, storage, and bandwidth, is increasingly becoming the infrastructure of choice for many organizations. As cloud offerings mature, service-based applications need to dynamically recompose themselves to self-adapt to changing QoS requirements. In this paper, we present a decentralized mechanism for such self-adaptation, using market-based heuristics. We use a continuous double-auction to allow applications to decide which services to choose, among the many on offer. We view an application as a multi-agent system and the cloud as a marketplace where many such applications self-adapt.

**ALGORITHM / METHODOLOGY:**

**DOMAIN: Software Engineering**

**IEEE REFERENCE: IEEE Paper on Software Engineering, 2013**



ISO / IEC 20000 CERTIFIED



BHARTIYA UDYOG  
RATAN - AWARDED



BITS PILANI  
PRACTICE SCHOOL



ISO 9001 : 2008 CERTIFIED



# AADHITYAA INFOMEDIA SOLUTIONS

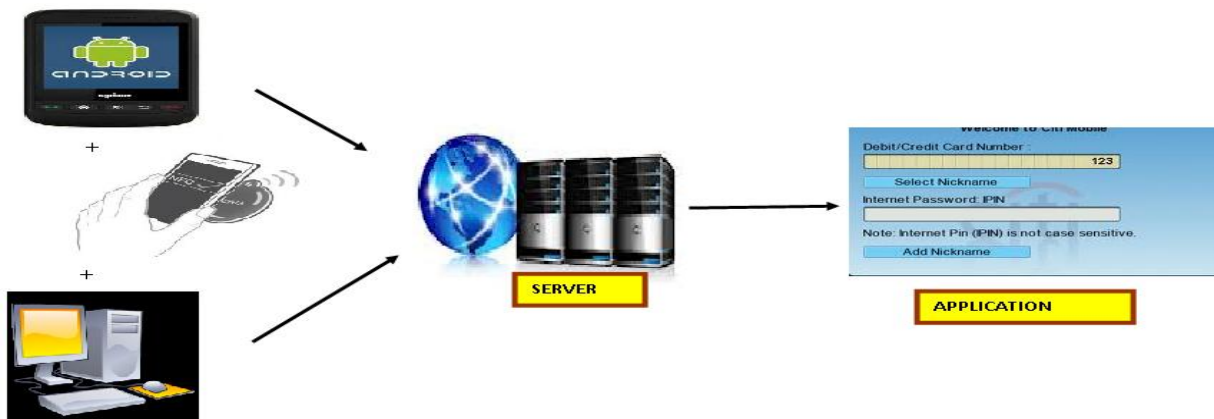
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6053. DYNAMIC HANDOFF & SESSION TRANSFER ON REGISTERED DEVICES FOR SECURED LAYER WEB TRANSACTIONS USING NFC

### ARCHITECTURE DIAGRAM



**DESCRIPTION:** In the **EXISTING SYSTEM**, we only allowed to access the application using multiple devices at a time. It sometimes provides the way to misuse the application. In the **PROPOSED SYSTEM**, user is allowed to register into the server by providing the details like Username, Password, NFC, Random Number, IP address (For System), IMEI & IMSI number (For Mobile) and Devices Information. The User can login to the Server by selecting any one of the device after authentication. During the application is in mid way, for some reason disconnection occurs then User can login via another device, the same process will be continued which means the session transfer will be achieved.

**ALGORITHM / METHODOLOGY:** Security Random Number Generation

**DOMAIN:** Android, Embedded, Security

**IEEE REFERENCE:** IEEE Paper on Advanced 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>
----------------------------------	---	--	----------------------------------



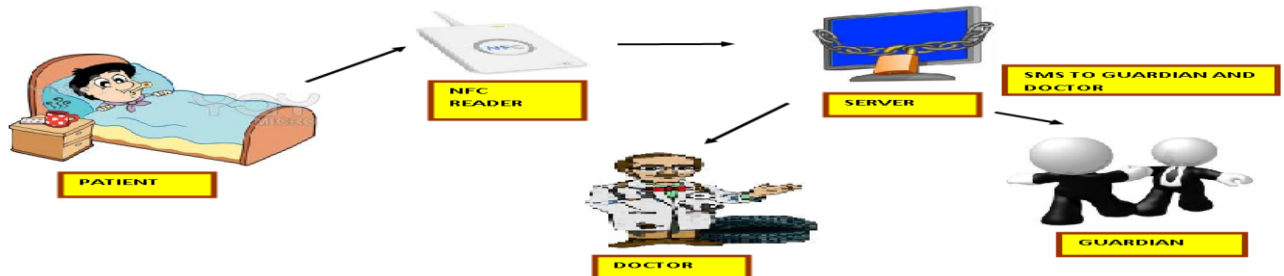
# AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6054. ANDROID AND NFC BASED REMOTE TELEMONITORING SYSTEM WITH EMERGENCY ALERT ARCHITECTURE DIAGRAM





**DESCRIPTION:** In the **EXISTING SYSTEM**, Age old People or sick people has to be monitored by Doctors manual or requires Guardian’s help to monitor their health. In the **PROPOSED MODEL**, Providing elderly people with a mobile-phone based patient terminal with NFC for Authentication and communication links to sensor devices. IF any abnormality is identified immediately supports are provided to save the life of the Patient. **MODIFICATION** that we propose is that the Generation of Automatic Alert SMS to the Patient’s Guardian in case of emergency

**ALGORITHM / METHODOLOGY:** Secure Random Key Generation

**DOMAIN:** Mobile Computing, Android, Security, Embedded

**IEEE REFERENCE:** IEEE TRANSACTIONS on Information Technology in Biomedicine, 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

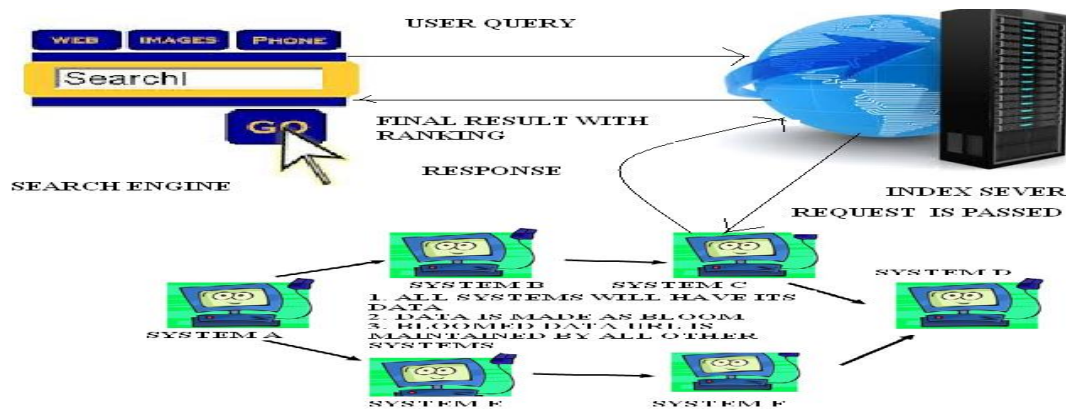
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6055 (DN 10045). 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

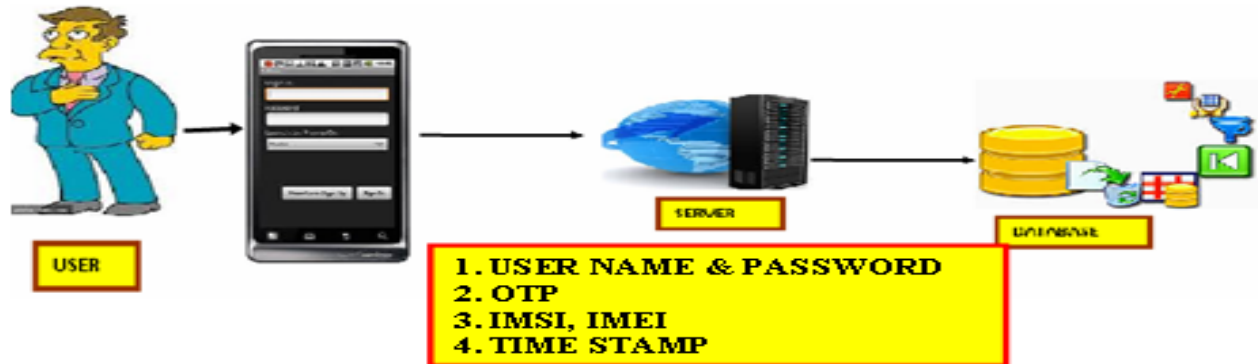
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6056. MOBILE BASED AUTHENTICATION SCHEME FOR SECURED DATA ACCESS

### ARCHITECTURE DIAGRAM

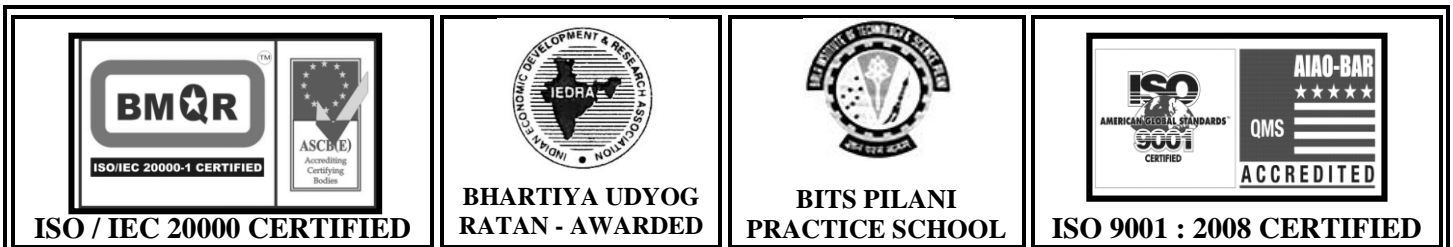


**DESCRIPTION:** In the **EXISTING SYSTEM**, we only use textual passwords when accessing the sensitive applications. But the textual passwords are easily hacked by the hackers. So those are vulnerable to attacks. In the **PROPOSED SYSTEM**, an Android Application is created in which user will be giving the Username and Password and send a request to generate an One Time Password (OTP) to the Server. Upon the received request, the Server generates a One Time Password which is Encrypted and send back to the User's Mobile. Then the User will be giving the Encrypted OTP along with their IMEI and IMSI number of their Mobile Phone and Time Stamp, only then concerned application will accessed by the User. **MODIFICATION** that we propose is GPRS is achieved rather SMS Technology, where Message delivery problems would happen.

**ALGORITHM / METHODOLOGY:** Random Key Generation

**DOMAIN:** Security

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







**AADHITYAA INFOMEDIA SOLUTIONS**

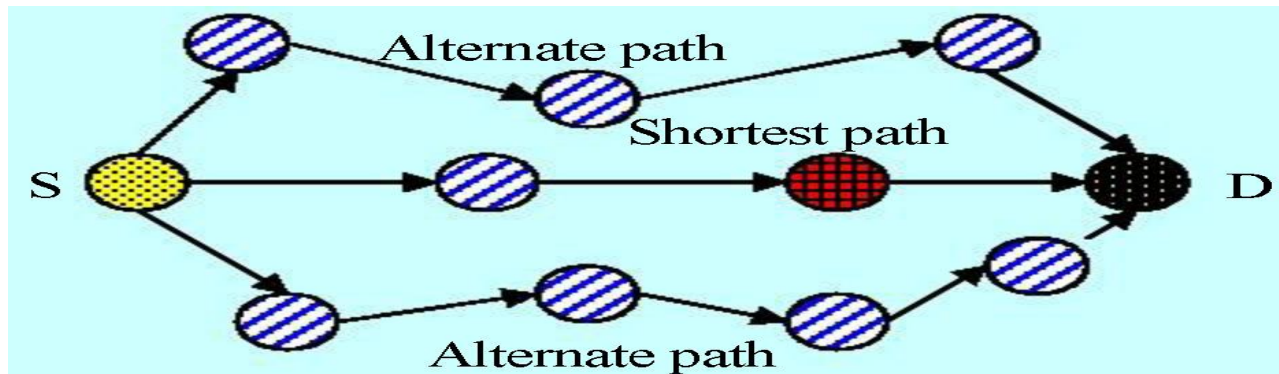
TRUST ME -  
CRISIL  
CERTIFIED

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



**JA 6057. DESIGN OF SECURED DATA COMMUNICATION  
WITH AVOIDANCE OF SHORTEST PATH**

**ARCHITECTURE DIAGRAM**






**DESCRIPTION:** In **EXISTING SYSTEM**, the hackers can perform the Man in Middle attack by identifying the shortest path and compromising them. So that they can hack the confidential data in the Wireless Sensor Networks. In the **PROPOSED SYSTEM**, we implement the Alternate Path Routing Algorithm to prevent the Intrusion. Here first we'll calculate the available path when a Source node is sending the data to the Destination. In the **MODIFICATION** Process, from the available paths we can randomly choose the path to send the data to destination node except using the Shortest Path in the Network. So that the attackers are not able to find identify the data transmission path. Also for Security Process, we can Encrypt the Data.

**ALGORITHM / METHODOLOGY:** Alternative Path Routing Algorithm

**DOMAIN:** Networking

**IEEE REFERENCE:** IEEE Paper on Computer Theory and Engineering, 2013

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



# AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6058. IDENTIFICATION OF BEST LOCATION ON USER'S MOBILITY BASED IN SIGNAL STRENGTH DIFFERNECE

### ARCHITECTURE DIAGRAM







**DESCRIPTION:** In the **EXISTING SYSTEM**, the popular location fingerprint, Received Signal Strength (RSS), is observed to differ significantly across different devices' hardware even under the same wireless conditions. The system was not that Effective when compared to SSD. In the **PROPOSED SYSTEM**, we are using, SSD Approach is used to Identify Best matched Tower from the user's point of Position. User's Signal Strength is calculated so that the difference of the Signal Strength between the user with the different Towers are analyzed to identify a best matched or nearest Tower from the user point of view. We present the results of two well-known localization algorithms (K Nearest Neighbor and Bayesian Inference) when our proposed fingerprint is used. **MODIFICATION** part that we propose in this Project is to stream Advertisement Campaigns if the user passes best matched Tower by calculating SSD.

**ALGORITHM / METHODOLOGY:** KNN-Query, SSD

**DOMAIN:** Mobile Computing

**IEEE REFERENCE:** IEEE Transactions on Mobile computing, 2013

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



# AADHITYAA INFOMEDIA SOLUTIONS

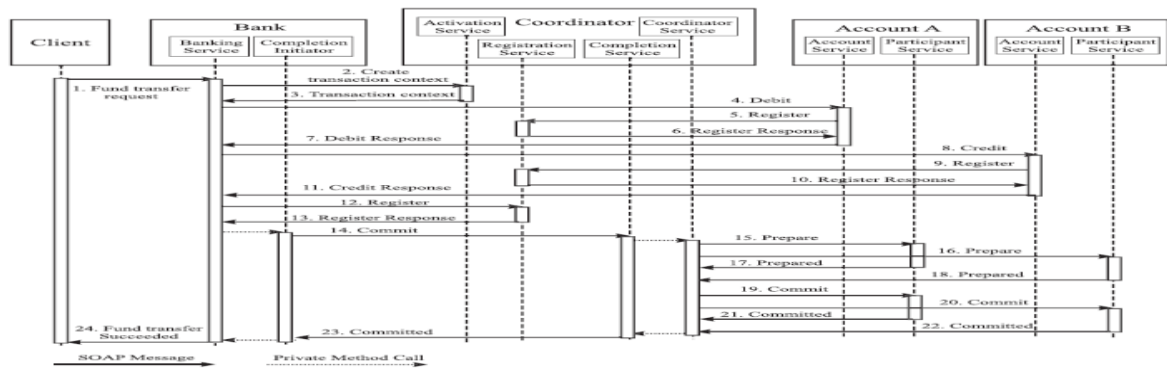
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6059 (DN 10046). 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

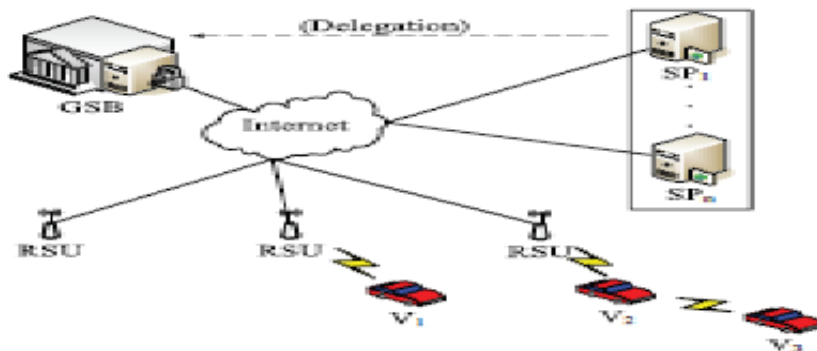
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6060. VVS: VANET VIDEO STREAMING- EFFECTIVE BROADCASTING AND PORTABLE BILLING

### ARCHITECTURE DIAGRAM:



**DESCRIPTION:** In the **EXISTING SYSTEM**, there is no effective service utilization was introduced in the VANETS. In the **PROPOSED SYSTEM**, User Request for a Internet Connectivity where request is passes to the Road Side Unit (RSU). RSU Communicates with to the Service Provider for accessing the Internet. In the **MODIFICATION SYSTEM**, where we are implementing the process of video request instead of Internet, Video Request is passed to the RSU and then to the Server. But the Major modification that we propose is that a Vehicle is Out Of Coverage Area, they may not be able to access the Server, in such conditions Videos can be streamed from another Vehicles of Uncoverage Vehicle can communicate.

### ALGORITHM / METHODOLOGY:

**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

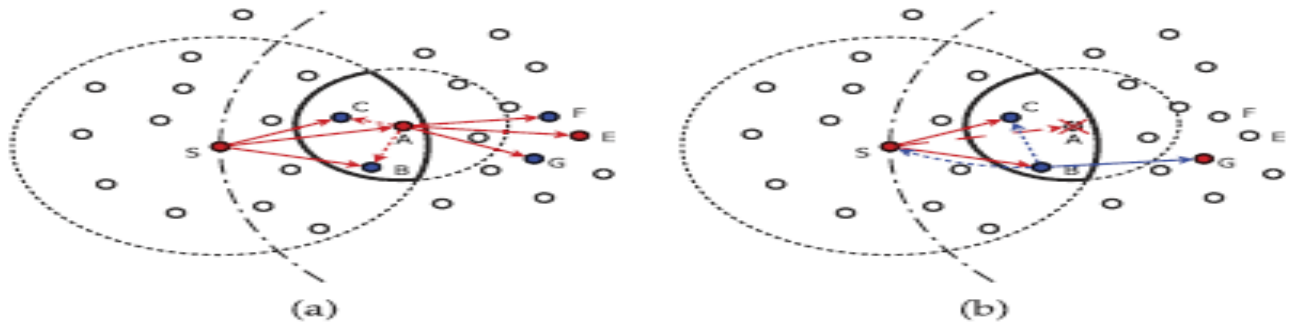
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6061. RELIABLE DATA DELIVERY WITH REDUCED ROUTING OVERHEAD IN MOBILE ADHOC NETWORKS

### ARCHITECTURE DIAGRAM



**DESCRIPTION:** In the **EXISTING SYSTEM**, due to the mobility of the nodes in MANETS, the Network faces a frequent link breakage problem which also leads to data loss. In the **PROPOSED SYSTEM**, we propose a neighbor coverage-based probabilistic rebroadcast protocol for reducing routing overhead in MANETs by which the a node can send the Route request to the other nodes till the destination is reached. So that the node can determine the exact path to send the data. In the **MODIFICATION PROCESS**, We are implementing an Next Hop Node Monitoring by which we can check whether the Next node is able to transmit the packet. If the any of the intermediate node leave the Network or Disconnected from the network, the data will transmitted to the Destination via Alternate Path Automatically. So that the Data can be effectively transmitted. Also for Security Purpose we are encrypting the data Packets during transmission.

**ALGORITHM / METHODOLOGY:** Neighbor Coverage-based Probabilistic Rebroadcast

**DOMAIN:** Mobile Ad-Hoc Networks

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



## JA 6062. ANDROID BASED CONTROL OF PORTABLE 3 AXIS PICK AND PLACE ROBOT

### ARCHITECTURE DIAGRAM



**DESCRIPTION:** In the **EXISTING SYSTEM**, we can only control the Robots in a Short distance Coverage. There is no remote mechanism was implemented to control the Robots from long distance. In the **PROPOSED SYSTEM**, we are implementing an Android Application by which we can control the Robot like Moving Forward, Backward, Right and Left directions. We can command the Robot to perform the Arm activities like Arm Up, Arm Down and Grabber Open and Grabber Close Operations. To implement this Concept, we have to enable the Server GPRS and Mobile GPRS and the Robot will be connected to the Server.

### ALGORITHM / METHODOLOGY:

**DOMAIN:** Android, Embedded and Robotics

**IEEE REFERENCE:** IEEE Paper on Industrial Technology, 2013



ISO / IEC 20000 CERTIFIED



BHARTIYA UDYOG  
RATAN - AWARDED



BITS PILANI  
PRACTICE SCHOOL



ISO 9001 : 2008 CERTIFIED



# AADHITYAA INFOMEDIA SOLUTIONS

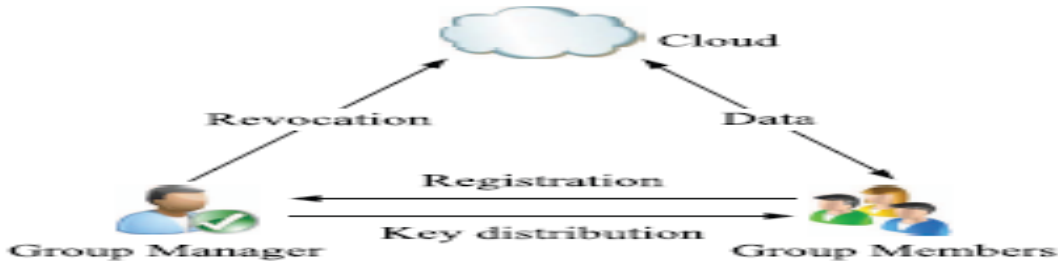
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6064 MULTI OWNER AUTHENTICATION SYSTEM, WITH ENCRYPTED SEURED DATA IN CLOUD COMPUTING

### ARCHITECTURE DIAGRAM:



**DESCRIPTION:** With the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. In this paper, we propose a secure multiowner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users.

### ALGORITHM / METHODOLOGY: BLS Signature Algorithm

**DOMAIN:** Cloud Computing, Security

**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

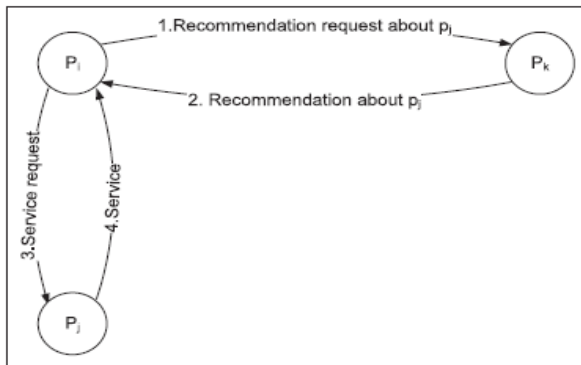
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6065 (DN 10034). 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

 <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

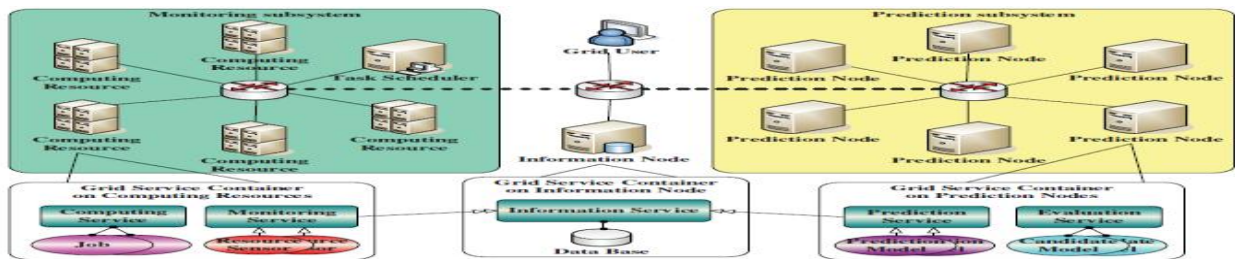
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6066 (DN 10044). 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

 <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

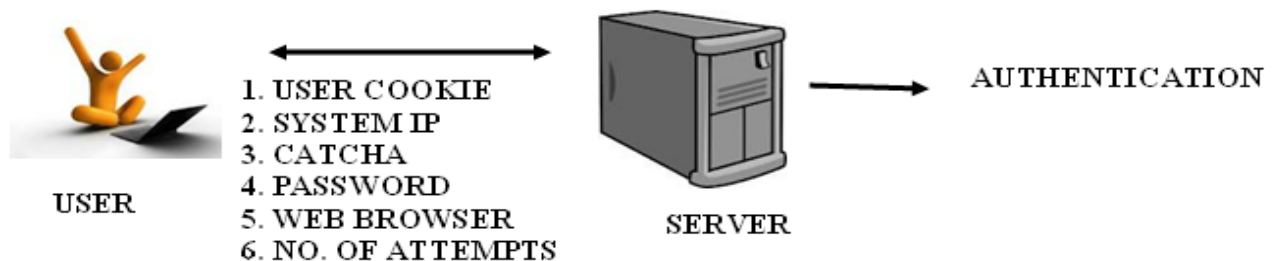
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6067 (DN 10047). 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 CERTIFIED</p>	 <p>BHARTIYA UDYOG RATAN - AWARDED</p>	 <p>BITS PILANI PRACTICE SCHOOL</p>	 <p>ISO 9001 : 2008 CERTIFIED</p>
--	---	---	--



# AADHITYAA INFOMEDIA SOLUTIONS

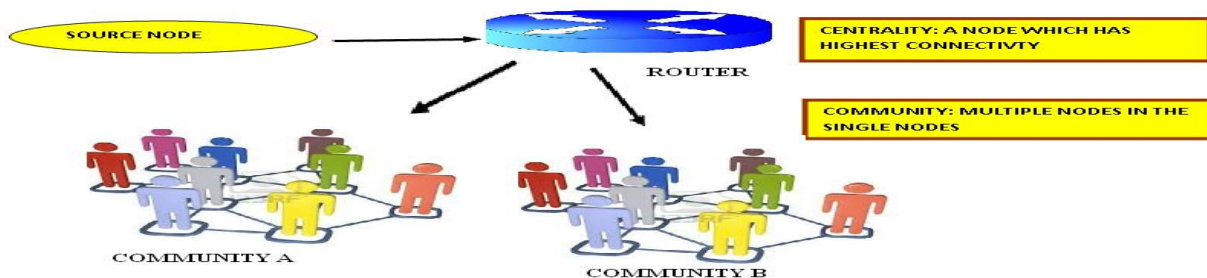
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6068 (DN 10048). 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

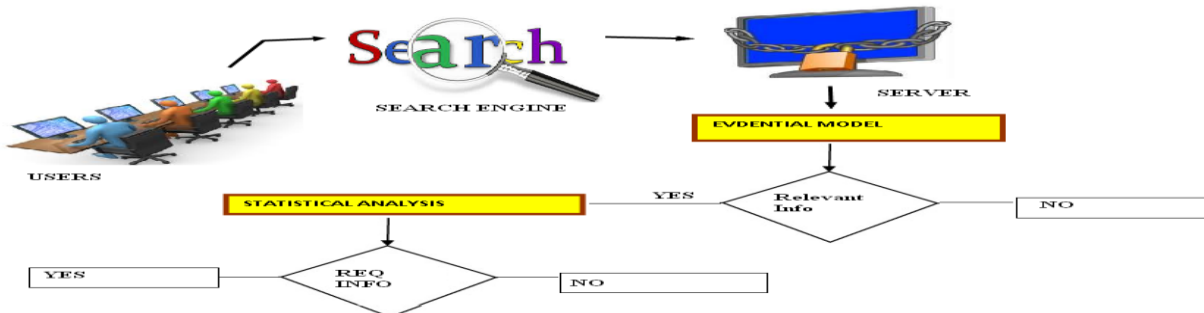
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6069 (DN 10049). 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

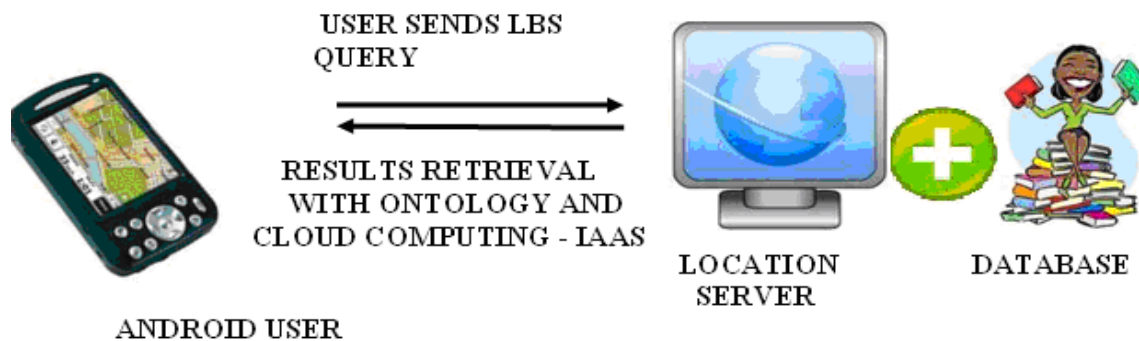
TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6070. ANDROID BASED LOCATION BASED SERVICES WITH ONTOLOGY & PROXY COMPUTATION WITH SECURITY

### ARCHITECTURE DIAGRAM



**DESCRIPTION :** In the **EXISTING SYSTEM**, the Queries are made by User Manually, which more time consuming and route is confusing. In the **PROPOSED MODEL**, Android and Cloud Computing are integrated. Android User makes a Query to the Cloud Server via Proxy Server. Data is verified its availability in proxy server first, only then the request if forwarded to the main cloud server in case of unavailability of data in the proxy server. if it is which has all the Location Information. We Implement Infrastructure as a service (IAAS) Ontology Process is also proposed. The **MODIFICATIONS** is made to have the privacy of the User's Location in which Query is requested. We use Three Layer of Security likely, High, Medium and Low for the Privacy implementation. We also Propose KNN Query Algorithm for Effective & Nearest Data Retrieval with respect to the user's (Android) location.

**ALGORITHM / METHODOLOGY:** KNN Query, EVR

**DOMAIN:** Data Mining, Android

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



**JA 6071. AN EMPIRICAL EVALUATION OF MUTATION  
TESTING FOR IMPROVING THE TEST QUALITY OF SAFETY-  
CRITICAL SOFTWARE  
ARCHITECTURE DIAGRAM**

**DESCRIPTION:** Testing provides a primary means for assuring software in safety-critical systems. To demonstrate, particularly to a certification authority, that sufficient testing has been performed, it is necessary to achieve the test coverage levels recommended or mandated by safety standards and industry guidelines. Mutation testing provides an alternative or complementary method of measuring test sufficiency, but has not been widely adopted in the safety-critical industry. In this study, we provide an empirical evaluation of the application of mutation testing to airborne software systems which have already satisfied the coverage requirements for certification. Specifically, we apply mutation testing to safety-critical software developed using high-integrity subsets of C and Ada, identify the most effective mutant types, and analyze the root causes of failures in test cases. Our findings show how mutation testing could be effective where traditional structural coverage analysis and manual peer review have failed. They also show that several testing issues have origins beyond the test activity, and this suggests improvements to the requirements definition and coding process.

**ALGORITHM / METHODOLOGY:**

**DOMAIN: Software Engineering**

**IEEE REFERENCE: IEEE Paper on Software Engineering, 2013**

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



# AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6072. NFC ON COGNITIVE SYSTEM FOR LOCATION BASED SERVICES USING ANDROID

In the **EXISTING SYSTEM**, the traditional museums have lot of olden and golden information's, which are seen by the visitors manually. The Visitor may miss some Good, Informative and Useful things, so the **PROPOSED SYSTEM** Speaks all about Integration of NFC Tag (Near Field Communication) with the Exhibits. User's mobile has NFC Reader which communicates with the Tag to get the Information's from the Exhibits. User will never miss out any Objects. In the **MODIFICATION PROCESS**, during Registration Process, Server will identify the User's Interest towards Text / Image / Video based Data Retrieval system. Based on it, Server will transmit the Data in that mode to the User.

**DOMAIN: Data Mining, Mobile Computing, Embedded, Android**

**IEEE REFERENCE: IEEE Paper on Near Field Communications, 2013**

## JA 6073. AN ADAPTIVE SYSTEM BASED ON ROADMAP PROFILLING IN VANETS

In the **EXISTING SYSTEM**, there is no automatic intimation mechanism was implemented to inform about the accident for the people who are all traveling in the same direction. So the following people will suffer a lot and it will more time to go via alternate route. In the **PROPOSED SYSTEM**, we implement Vehicular Adhoc Networks for the effective communication between vehicles. We implement three major mechanisms 1. Full Dissemination in which the information is passed to all the vehicles in the straight line. 2. Regular Dissemination in which some parts of cross lanes are present, so Dissemination or Data transfer will be reduced. 3. More Complex in which lots of cross lanes are present, so Data dissemination is poor. The **MODIFICATION** which we propose is that if one vehicle is in a out of Coverage Area, Data dissemination is archived automatically if it reaches the Coverage Area.

**DOMAIN: Vehicle Ad-Hoc Networks**

**IEEE REFERENCE: IEEE Paper on Networking, 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 (1<sup>ST</sup>) ISO 20000, SEI CMMI LEVEL 3  
COMPLIANCE & ISO 9001 : 2008 CERTIFIED  
SOFTWARE DEVELOPMENT COMPANY)



## JA 6074. AUTOMATIC USER DETECTION, SCHEDULING AND ANDROID BASED HOME AUTOMATION SYSTEM

In the **EXISTING SYSTEM**, the control of Electrical Appliances would happen manually; there is no Automatic and Remote / Wireless Dimming implementation. In the **PROPOSED** user can control the Appliances from the Remote Place using Zigbee Technology. User can control all Appliances at a time like ON / OFF, can also Control one by one. User can also dim the PWM Light from full Brighter till less Illumination. User can also control Half Tone / Full tone. We also implement Scheduler Process in which Devices are controlled in a Sequence. In the Automatic Mode, the Devices are Controlled depends on the availability of a person.

**DOMAIN:** Android, Embedded and Security




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

## AJA 1. DESIGN OF REMOTE NETWORK MONITORING AND CONTROL SYSTEM FOR ANDROID

In the **EXISTING SYSTEM**, the main problem is most Smart phone is having poor battery when application for intensive connectivity services. In the **PROPOSED MODEL**, this paper speaks all about the comparative study between 3G and Wifi only. In the implementation / **MODIFICATION** part, we develop a android based application where by remote server monitoring is achieved. Admin can guess the server from remote place and can visualize number of client machine switch ON. Admin can send unicast / multicast data from android phone. Admin can also shutdown / restart / logout a particular machine use android application.

**DOMAIN:** Android, Mobile Computing

**IEEE REFERENCE:** IEEE Paper on Information Society, 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 (1<sup>ST</sup>) ISO 20000, SEI CMMI LEVEL 3  
COMPLIANCE & ISO 9001 : 2008 CERTIFIED  
SOFTWARE DEVELOPMENT COMPANY)



## AJA 2. ANDROID BASED GREEN HOUSE MONITORING AND CONTROLLING USING AUTOMATIC & MANUAL METHODS

In the **EXISTING SYSTEM**, it is difficult to control indoor humidity. It is also difficult in monitoring and control of green house. In the **PROPOSED MODEL**, we are monitoring humidity in green house is too dry then the motor of water sprayer is activated. If green house is too humid the roof top of the green house is opened. In the **MODIFICATION** both manual and automatic is activated using android app. In the automatic mode control of water sprayer and opening of roof door is achieved automatically as per the humidity level. In the manual mode, all the controls are achieved by manual process.

**DOMAIN:** Android, Mobile Computing, Embedded

**IEEE REFERENCE:** IEEE Paper on QiR, 2013

## AJA 3. DEVELOPMENT OF SECURED SENSITIVE DATA TRANSMISSION OVER CLOUD

In the **EXISTING SYSTEM**, E- health has less security and cannot access the medical records in wireless medium. In the **PROPOSED MODEL**, cloud computing based Infrastructure As A Service (IAAS) is deployed for medical records data storage. Parent's records are stored in the server, whenever the android mobile user request the data, image as well as records are transmitted via GPRS connection. The medical data is encrypted using ECC algorithm for security purpose. In the **MODIFICATION** phase, medical related queries are by android user are processed and answered by the server. We use stemming algorithm for filtering.

**ALGORITHM / METHODOLOGY:** Elliptical Curve Cryptography Algorithm

**DOMAIN:** Android, Mobile Computing, Cloud Computing

**IEEE REFERENCE:** IEEE Paper on Communication & Signal Processing, 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 (1<sup>ST</sup>) ISO 20000, SEI CMMI LEVEL 3  
COMPLIANCE & ISO 9001 : 2008 CERTIFIED  
SOFTWARE DEVELOPMENT COMPANY)



## AJA 4 (DN 10050). 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

## AJA 5. ANDROID BASED GREEN COMPUTING FOR EFFECTIVE POWER UTILISATION & LOAD MANAGEMENT

In the **EXISTING SYSTEM**, we use manual method to control the devices that are present in are home. There is no automatic mechanism was implemented to control the devices using Mobile Applications. In the **PROPOSED SYSTEM**, an Android Application is created where User can Select Manual\Automatic control of the Devices. In the Manual Control, User can control the Devices Manually. In the Automatic mode the User can select the Device along with the Device Running Time. The Server will schedule the running of the Device based on the Non peak hours automatically in order to equalize the load of the Machine.

**ALGORITHM / METHODOLOGY:** Distributed Scheduling Algorithm

**DOMAIN:** Android, Security and Embedded

**IEEE REFERENCE:** IEEE Transactions on Smart Grid, 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 (1<sup>ST</sup>) ISO 20000, SEI CMMI LEVEL 3  
COMPLIANCE & ISO 9001 : 2008 CERTIFIED  
SOFTWARE DEVELOPMENT COMPANY)



## AJA 6. CONGESTION-AWARE SPATIAL ROUTING IN HYBRID HIGH-MOBILITY WIRELESS MULTIHOP N/WS

We develop a spatial framework to provide end-to-end delay estimates and guarantees in mobile multihop networks. The novel aspect of this approach is the attribution of network and MAC layer congestion to space, which enables congestion-aware routing and provides delay guarantees over a much longer duration than that achieved by the routing algorithms based on individual nodes. In a mathematically rigorous setting, first, we prove that over the duration during which the node density and the traffic pattern remain stationary, the expected values of local congestion and end-to-end delay roughly remain invariant. Second, we present an accurate method of delay estimation over geographic paths, namely path integration, and derive an upper bound for its estimation error.

**ALGORITHM / METHODOLOGY:** Source Routing Algorithm

**DOMAIN:** Mobile Computing

**IEEE REFERENCE:** IEEE Transactions on Mobile Computing, 2013

## AJA 7. VEHICLE ANTI-THEFT TRACKING SYSTEM BASED ON INTERNET OF THINGS

In the **EXISTING SYSTEM**, there is no very effective system to track the stolen vehicles, still police job is finding the lost vehicle is very difficult. In the **PROPOSED MODEL**, GPS (Global Positioning System), GSM and RFID are connected to the vehicle. If the vehicle is stolen, owner would SMS "Where" to the GSM connected to the vehicle hardware, immediately location of vehicle is send to the android owner. Owner can stop the vehicle through GPRS. In the **MODIFICATION**, car door is controlled using Android application.

**ALGORITHM / METHODOLOGY:** Google Earth Service, Decoding Algorithm

**DOMAIN:** Android, Mobile Computing

**IEEE REFERENCE:** IEEE Paper on ICVES, 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 (1<sup>ST</sup>) ISO 20000, SEI CMMI LEVEL 3  
COMPLIANCE & ISO 9001 : 2008 CERTIFIED  
SOFTWARE DEVELOPMENT COMPANY)



## AJA 8. 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 (1<sup>ST</sup>) ISO 20000, SEI CMMI LEVEL 3  
COMPLIANCE & ISO 9001 : 2008 CERTIFIED  
SOFTWARE DEVELOPMENT COMPANY)**



## IEEE 2012 PROJECT LIST

### JA 6075. STUDENT BEHAVIOR & ATTENDANCE MONITORING WITH AUTOMATIC SMS ALERT TO PARENTS

DOMAIN: Mobile Computing, Embedded

### JA 6076. ANDROID BASED MOVING OBJECTS DETECTION WITH ALERT SMS WITH IMAGE STREAMING

DOMAIN: Mobile Computing, Android

### JA 6077. ASSURING SECURED & DEPENDABLE CLOUD STORAGE SERVICES WITH ERASURE CODE TECHNIQUE

DOMAIN: Cloud Computing, Security

### JA 6078. IDENTIFICATION, DETECTION AND REMOVAL OF INTRUSION ATTACKS IN MULTITIER WEB APPLICATIONS

DOMAIN: Network Security

### JA 6079. M – GUARDIAN: ANDROID BASED ELDERLY PEOPLE ACTIVITY AND HEALTH MONITORING USING CLOUD

DOMAIN: Cloud Computing, Android, Embedded



ISO / IEC 20000 CERTIFIED



BHARTIYA UDYOG  
RATAN - AWARDED



BITS PILANI  
PRACTICE SCHOOL



ISO 9001 : 2008 CERTIFIED



# AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6080. PREVENTION OF DDOS ATTACKS USING PORT NUMBER REVOLUTIONIZE & TIME STAMP – CLOCK DRIFTS

DOMAIN: Network Security

## JA 6081. AUTONOMOUS SPECTRUM HANDOFF FRAMEWORK IN ADHOC NETWORK WITH DYNAMIC LOAD BALANCING

DOMAIN: Mobile Computing

## JA 6082. IDENTIFICATION OF MALICIOUS PACKET LOSS DURING ROUTING MISBEHAVIOUR IN DTN

DOMAIN: Network Security

## JA 6083. EFFICIENT, DISTRIBUTED PEER TO PEER INTERACTIVE VOD STREAMING USING CHUNKING MECHANISM

DOMAIN: Networking

## JA 6084. SECURED DATA SHARING WITH ACCESS PRIVILEGE POLICIES AND DISTRIBUTED ACCOUNTABILITY IN CLOUD

DOMAIN: Cloud Computing, 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 (1<sup>ST</sup>) ISO 20000, SEI CMMI LEVEL 3  
COMPLIANCE & ISO 9001 : 2008 CERTIFIED  
SOFTWARE DEVELOPMENT COMPANY)



## JA 6085. DATA HIDING AND SECURED DATA STORAGE WITH ACCESS CONTROL TOWARDS MULTIPARTY PROTOCOLS

DOMAIN: Data Mining, Security

## JA 6086. DETECTION AND FILTERING SPAMS WITH CONTENT, EXTENSION AND ACTIVITY MONITORING

DOMAIN: Network Security

## JA 6087. EFFECTIVE UNMANNED, AUTOMATIC ROBOT CONTROL SYSTEM FOR EDUCATIONAL SOCIAL CAUSE

DOMAIN: Mobile Computing, Data Mining, Embedded

## JA 6088. A MACHINE BASED ANALYTIC APPROACH WITH SVM CLASSIFIER FOR FILTERING MOVIE AND PRODUCT QUALITY USING ANDROID SMART PHONE

DOMAIN: Mobile Computing, Android, Data Mining



ISO / IEC 20000 CERTIFIED



BHARTIYA UDYOG  
RATAN - AWARDED



BITS PILANI  
PRACTICE SCHOOL



ISO 9001 : 2008 CERTIFIED



# AADHITYAA INFOMEDIA SOLUTIONS

TRUST ME -  
CRISIL  
CERTIFIED

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



## JA 6089. ANDROID BASED HOME SECURITY DOOR CONTROL WITH HUMAN DETECTION & IMAGE STREAMING, SMS

DOMAIN: Mobile Computing, Security, Embedded, Android

## JA 6090. VISUAL CRYPTOGRAPHY IMPLEMENTATION WITH KEY SHARING FOR EFFECTIVE PHISHING DETECTION PROCESS

DOMAIN: Web Security, Mobile Computing



## JA 6091. THEMIS: A MUTUALLY VERIFIABLE BILLING SYSTEM FOR THE CLOUD COMPUTING ENVIRONMENT

DOMAIN: Cloud Computing, Security

## JA 6092. EFFECTIVE IMPLEMENTATION OF TRUST WORTHY CO ORDINATION IN INTER COMMUNICATION WEB SERVICE

DOMAIN: Web Service

# 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>
--	---	---	--