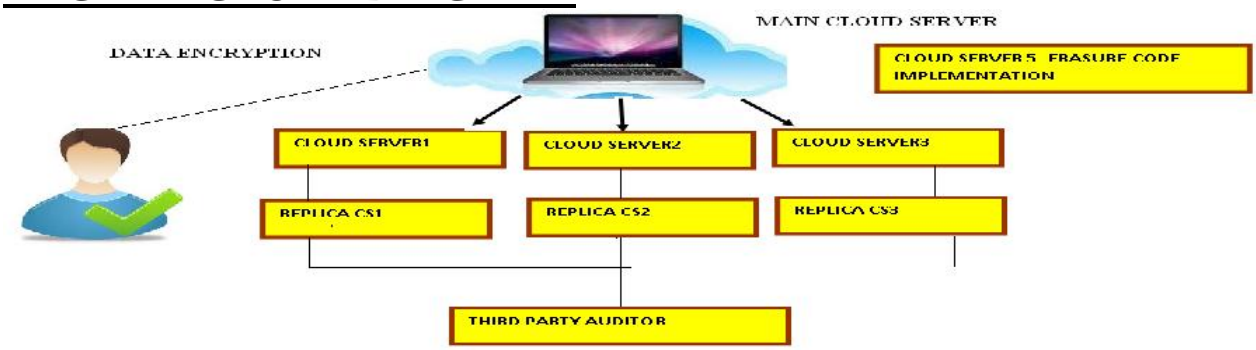
PROJECTS IN DOTNET / ANDROID

DNAP 1001. (J2EAP 11001). ASSURING SECURED & DEPENDABLE CLOUD STORAGE SERVICES WITH ERASURE CODE TECHNIQUE

ARCHITECTURE DIAGRAM

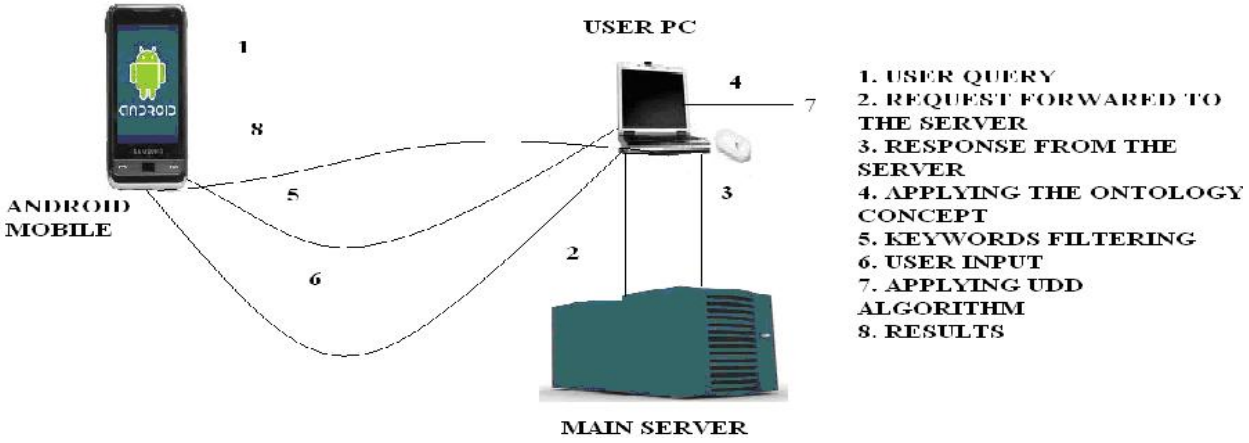


DESCRIPTION : In the **EXISTING SYSTEM**, there is no big security provided in the Cloud server for data safety. If at all security exists, the third party auditor should be allowed to access the entire data packets for verification. In the **PROPOSED SYSTEM**, Cloud server spilt the file into batches and allowed for encryption. The corresponding encrypted batches are kept in different Cloud servers and their keys are distributed in different key server. These encrypted batches are kept in replica servers as a backup. This encrypted data are converted into bytes and added parity bit process by the data owner in order to restrict TPA by accessing the original data. The Cloud server generates the token number from the parity added encrypted data and compared with the signature provided to the TPA to verify the Data Integrity. We also implement Erasure Code for the back-up of the data. The **MODIFICATION** that we propose is the encryption process of the data by the data owner before it reaches the Cloud server.

DOMAIN: Cloud Computing, Security

DNAP 1002. (J2EAP 11002). ANDROID BASED EFFECTIVE AND EFFICIENT SEARCH ENGINE RETRIEVAL SYSTEM USING ONTOLOGY

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 us 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.

DOMAIN: Mobile Computing, Android, Data Mining

DNAP 1003. (J2EAP 11004). DEVELOPMENT OF SECURITY SCHEME IN RELATIONAL DATABASES USING JTAM FOR THE DETCETION OF IDS

ARCHITECTURE DIAGRAM

DESCRIPTION : In the **EXISTING SYSTEM**, Relational database which has lot of Administrators to Control Every Tables. Admin is authorized to control their own Corresponding Tables only. If the admin password is hacked, then Data Changes and Updations can be Proceeded by the Hacker himself. There is no security factor. So **PROPOSED MODEL** Verifies the Policy Matching which deals with the Permitted Privileges of Every Admin and Joint Threshold Administration Model [JTAM] which aims at getting their Part of Session Key as Approval if one Admin is Updating the Data. The Session key Provided by all the Admins are integrated and Compared with the Original Session Key, only if the Key is matched Data is Modified. The **MODIFICATION** that we propose is by generating the Session Key and every part of the Key is sent as SMS to the Corresponding Admin's Mobile.

DOMAIN: Data Mining

DNAP 1004. (J2EAP 11005). AUTOMATIC IDENTIFICATION OF DISEASE TREATMENT WITH TRUST WORTHY RESULT'S USING MACHINE LEARNING APPROACH

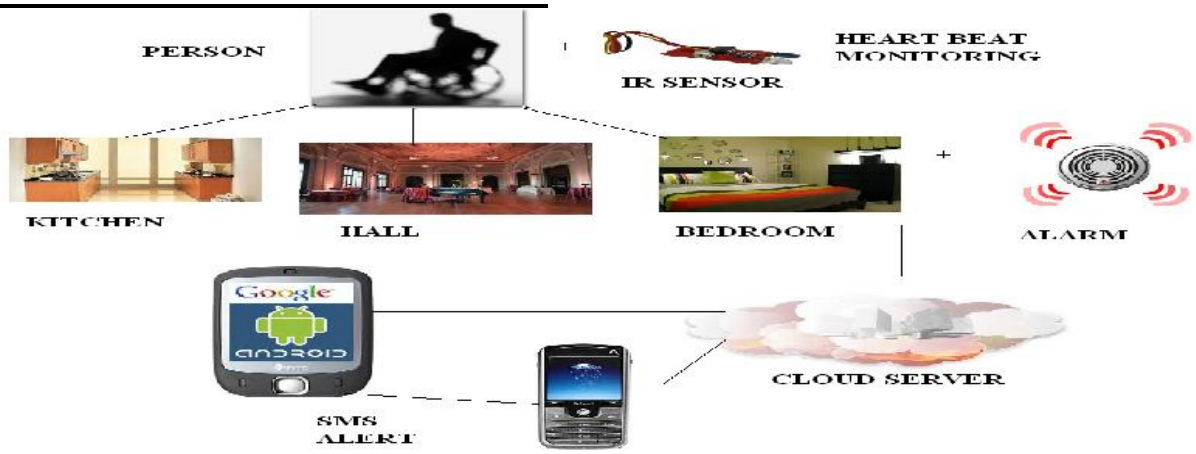
ARCHITECTURE DIAGRAM

DESCRIPTION : In the **EXISTING SYSTEM**, Internet Provides lot of Irrelevant / Useless / False Information's for the Disease Related Searches, which is more harmful. In the **PROPOSED SYSTEM** the Machine Learning Technique is introduced. This process Extracts the Information from the Published Medical Papers for the Queries given by the User. Classifiers are used to Identify Symptoms, Cure, Treatment and Side effects of any Disease and for its Treatment. This Project Extracts Truth and Trust over Medical Field. The **MODIFICATION** that we propose is the Ranking of Keywords present in a Medical Journals. The Ranking is achieved by calculating Term Frequency (No. of Occurrence) of User Searched Term with the Total Number of Filtered Key Words using Stemming, Ranking Algorithms.

DOMAIN: **Data Mining**

DNAP 1005. (J2EAP 11006). M – GUARDIAN: ANDROID BASED ELDERLY PEOPLE ACTIVITY AND HEALTH MONITORING USING CLOUD COMPUTING

ARCHITECTURE DIAGRAM



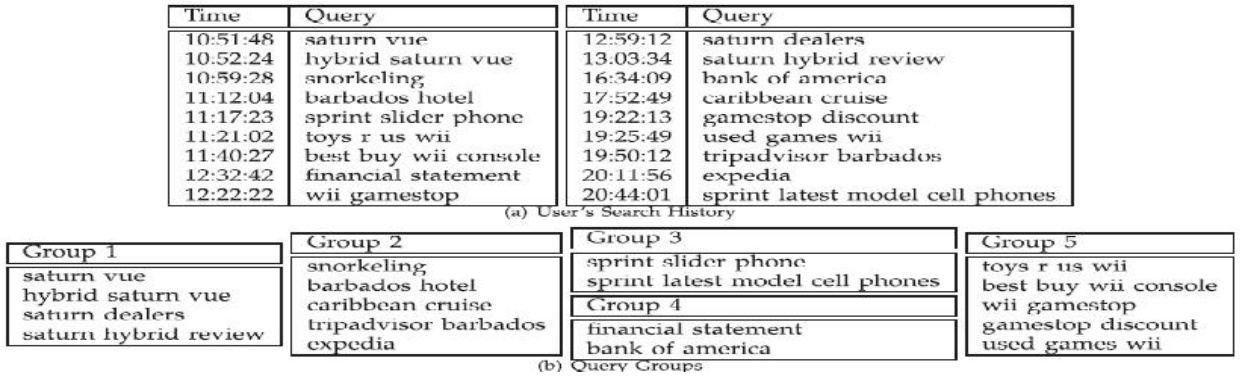
DESCRIPTION : In the **EXISTING SYSTEM,** there should be some Care Taker along with the Patient who personally monitor the Age Old Patients. In the **PROPOSED SYSTEM**, Smart home is regarded as an independent healthy living for elderly person. Advances in phone technology and new style of computing paradigm (i.e., cloud computing) permits real time acquisition, processing, and tracking of activities in smart home. In this paper, we develop android smart phone application to assists elderly people for independent living in their own homes. Smart phone application communicates with cloud through web server and assists the elderly person to complete their daily life activities. This is used to Track the Patient's Activity

along with the Remainders of Medicines, Food and other Activities. **MODIFICATION** that we propose is to monitor the Heart Beat of the Patient to find the normal functionality of the Patient along with IR based Tracking Solution at every room.

DOMAIN: Cloud Computing, Android, Embedded

DNAP 1006. (J2EAP 11007). EFFECTIVE RE-RANKING WITH ORGANIZING USER HISTORY, FEEDBACK AND ELIMINATION OF DUPLICATE RECORDS

ARCHITECTURE DIAGRAM



Time	Query	Time	Query
10:51:48	saturn vue	12:59:12	saturn dealers
10:52.24	hybrid saturn vue	13:03.34	saturn hybrid review
10:59:28	snorkeling	16:34:09	bank of america
11:12:04	barbados hotel	17:52:49	caribbean cruise
11:17:23	sprint slider phone	19:22:13	gamestop discount
11:21:02	toys r us wii	19:25:49	used games wii
11:40:27	best buy wii console	19:50:12	tripadvisor barbados
12:32:42	financial statement	20:11:56	expedia
12:22:22	wii gamestop	20:44:01	sprint latest model cell phones

(a) User's Search History

(b) Query Groups

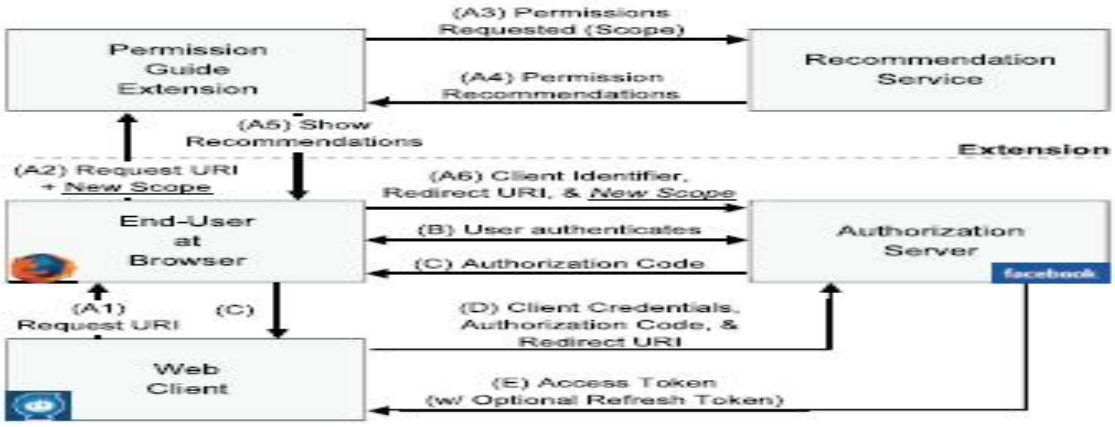
DESCRIPTION : In the **EXISTING SYSTEM**, users query request is Handled and resultant URLs are provided based on the user's hits into a URL. The searching process happens based on the Exact keyword matched in the metatag in the Corresponding URLs. In the **PROPOSED SYSTEM**, we're organizing the user's search history by categorizing the keywords, synonyms or same meaning words into same category and also we monitor, user's selection of the URLs for the corresponding queries. We segregate the same pattern of queries from different users and compare the entire selection URLs. This process helps to Re-Rank the

most often selected URLs by different user's to a new users who googles the same queries. The **MODIFICATION** we propose is getting the feedback from the users about the corresponding URLs which helps to Re-Rank resultant URLs in a more perfect manner. We Calculate the Positive feedback ratio to judge real best URL at the top of the site.

DOMAIN:. Data Mining

DNAP 1007. (J2EAP 11008). EFFECTIVE COLLABORTIVE FILTERING OF RECOMMENDATION SERVICES BASED ON OPEN AUTHORIZATION WITH SMS ALERT

ARCHITECTURE DIAGRAM



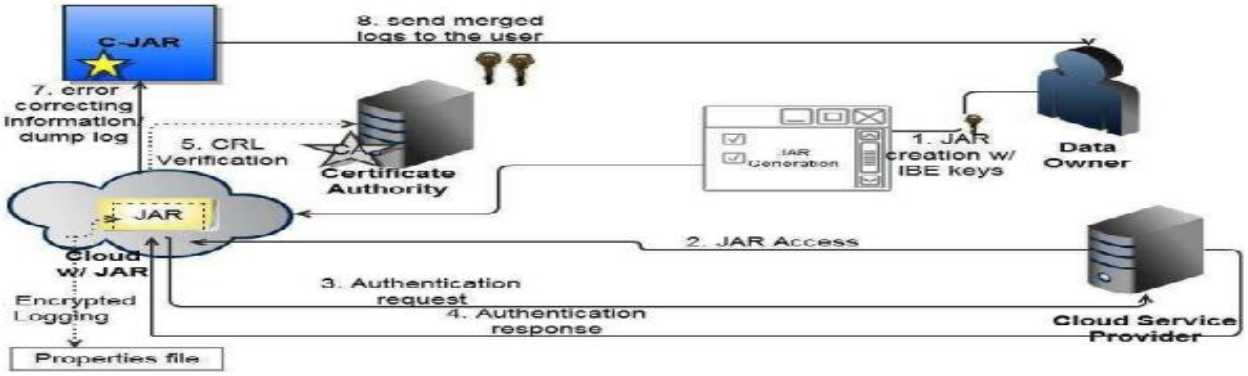
DESCRIPTION : In the **EXISTING SYSTEM**, Major online platforms such as Facebook, Google, and Twitter allow third-party applications access without User's Authorization. But, Such accesses must be authorized by users at installation time. In the **PROPOSED SYSTEM** a multi criteria recommendation model that utilizes application-based,

user-based, and category-based collaborative filtering mechanisms. Our collaborative filtering mechanism is effective by getting the authorization of the privileges from the user to access their database by the Third Party Applications via Recommendation Service and Permission Guide. Token number based Authentication process is used to verify the Third Party Applications. The **MODIFICATION** that we propose is to send the token number via Mobile SMS alert.

DOMAIN:. Web Security

DNAP 1008. (J2EAP 11014). SECURED DATA SHARING WITH ACCESS PRIVILEGE POLICIES AND DISTRIBUTED ACCOUNTABILITY IN CLOUD COMPUTING

ARCHITECTURE DIAGRAM



DESCRIPTION : In the **EXISTING SYSTEM**, A major feature of the cloud services is that users' data are usually processed remotely in unknown machines that users do not own or operate. While enjoying the convenience brought by Cloud Computing, users' fears of losing

control of their own data (particularly, financial and health data) can become a significant barrier to the wide adoption of cloud services. In the **PROPOSED SYSTEM**, Data Owner can upload the data into cloud server after encryption. User can subscribe into the cloud server with certain access policies such Read, Write and Copy of the Original Data. Logger and Log Harmonizer will a track of the access logs and reports to the Data Owner. This Access ensures Security. In the **MODIFICATION**, Automatic reporting of illegal action performance of any user to the data owner, as well as data owner would generate the random numbers set for the every user. So if the user entering into the account has to provide random number set, that will be verified by server.

DOMAIN: Cloud Computing, Security

DNAP 1009. (J2EAP 11015). DATA HIDING AND SECURED DATA STORAGE WITH ACCESS CONTROL TOWARDS MULTIPARTY PROTOCOLS

ARCHITECTURE DIAGRAM

Name	Sex	Nation	Salary
q1	F	England	>40K
q2	M	Canada	≤40K
q3	M	USA	≤40K
q4	F	Peru	≤40K

T_σ

Name	Sex	Nation	Salary
q1	F	*	>40K
q2	M	*	≤40K
q3	M	*	≤40K
q4	F	*	≤40K

T^*_σ

Name	Sex	Nation	Salary
q1	F	EU	>40K
q2	M	AM	≤40K
q3	M	AM	≤40K
q4	F	AM	≤40K

Name	Sex	Nation	Salary
q5	M	Canada	>40K
q6	M	USA	>40K
q7	F	Brazil	>40K
q8	F	Italy	≤40K

Name	Sex	Nation	Salary
q5	M	*	>40K
q6	M	*	>40K
q7	F	*	>40K
q8	F	*	≤40K

Name	Sex	Nation	Salary
q5	M	AM	>40K
q6	M	AM	>40K
q7	F	AM	>40K
q8	F	EU	≤40K

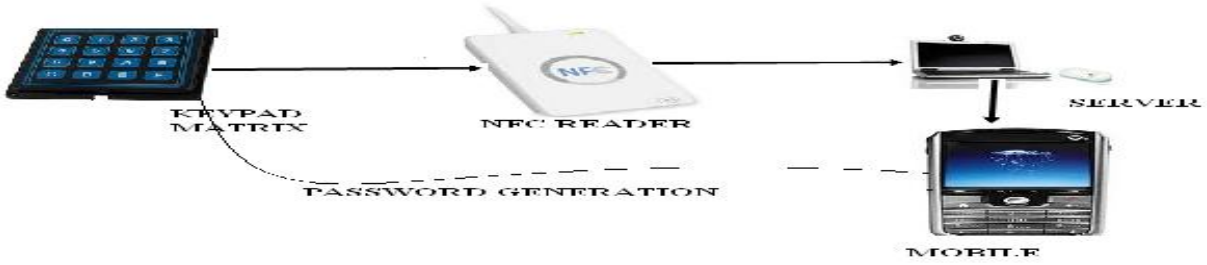
DESCRIPTION : In the **EXISTING SYSTEM**, there is no Security Scheme operated for Data Storage Services between Multi Party protocols. In the **PROPOSED SYSTEM**, a look-ahead approach, specifically for secure multiparty protocols to achieve distributed k-anonymity,

which helps parties to decide if the utility benefit from the protocol is within an acceptable range before initiating the protocol. The look-ahead operation is highly localized and its accuracy depends on the amount of information the parties are willing to share. The system deals with Generalization approach, with hiding the Employment Department with a common Identify along with hiding the Exact Salary, Suppression Approach Hiding User Name along with their Country Identity. In the **MODIFICATION**, a Authentication Key is Generated before a user change / update the data for Verification. Entire Data is encrypted to ensure Security.

DOMAIN: Data Mining, Security

DNAP 1010. (J2EAP 11016). ANALYSTIC APPROACH TO DETECT ATM COUNTERFEIT CARDS USAGE USING NFC TECHNOLOGY

ARCHITECTURE DIAGRAM



DESCRIPTION : In the **EXISTING SYSTEM,** People relish the flexibility of being able access their monetary assets when and where they need them. The abundance of cards able to withdraw funds from Automatic Teller Machines (ATMs) has not gone unnoticed by the cyber criminal element. Means for skimming and cloning cards exist and the market continues to grow. In the **PROPOSED SYSTEM**, Server Tracks the Same ATM Card's Usability in different ATM

Machine locations or accessibility of the same Card more times in a single ATM Machine. **MODIFICATION** that we Propose NFC Card is used as ATM Card. If the same Card is used in different ATM Machines at the same Time, the Server detects it as Attack so that the ATM Card is blocked and Alert SMS is send to the Legitimate User's Mobile Number. For every new Transaction a Token is generated as SMS to the user's Mobile so that user can write in the NFC Card which is verified for Authentication. This process will surely prevent the accessibility of ATM Card even Attacker steals the ATM Card.

DOMAIN: Mobile Computing, Embedded

DNAP 1011. (J2EAP 11018). EFFECTIVE UNMANNED, AUTOMATIC ROBOT CONTROL SYSTEM FOR EDUCATIONAL SOCIAL CAUSE – LIBRARY SYSTEM

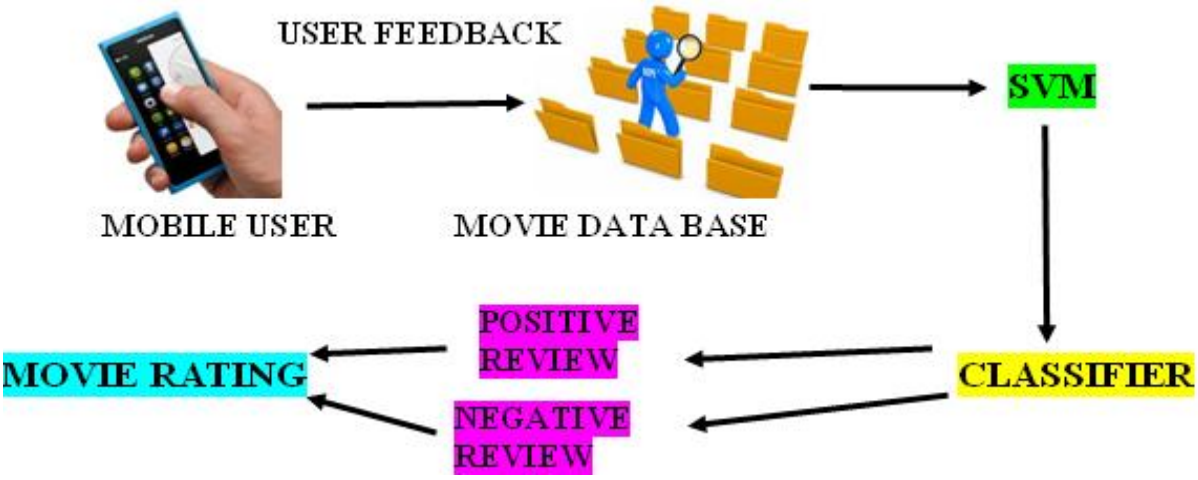
ARCHITECTURE DIAGRAM

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.

DOMAIN: Mobile Computing, Data Mining, Embedded

DNAP 1012. (J2EAP 11019). A MACHINE BASED ANALYTIC APPROACH WITH SVM CLASSIFIER FOR FILTERING MOVIE AND PRODUCT QUALITY USING ANDROID SMART PHONE

ARCHITECTURE DIAGRAM

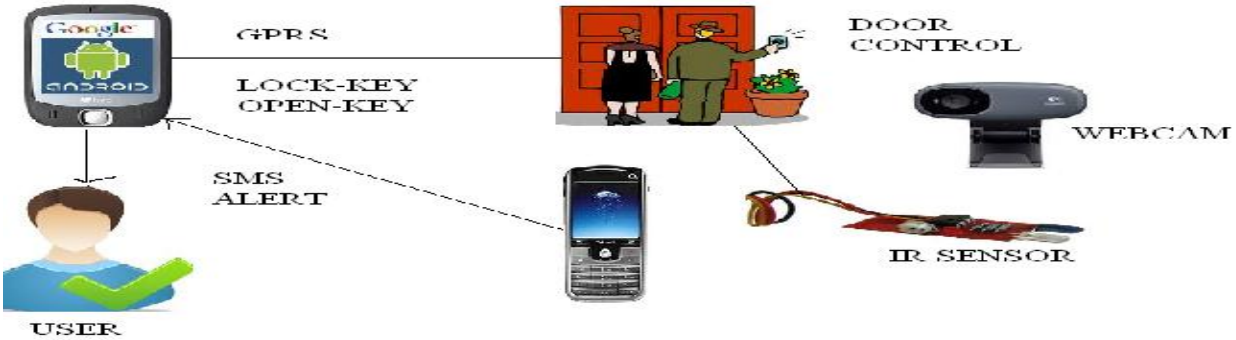


DESCRIPTION : In **EXISTING SYSTEM**, computer based movie rating process happens, that too no proper rating is happening. In the **PROPOSED SYSTEM**, we use the Android based user feedbacks are about only movie is obtained using SVM technique and feature based extraction method. User can select the feature and can provide positive and negative feedback. We use steaming algorithm to extract the proper feedback. In the **MODIFICATION**, User id is provided by verifying the mobile number, so it can avoid same user's re-feedback provision. We also provide same implementation for product review also.

DOMAIN: Mobile Computing, Android, Data Mining

DNAP 1013. (J2EAP 11020). ANDROID BASED HOME SECURITY DOOR CONTROL WITH HUMAN DETECTION AND IMAGE STREAMING WITH SMS ALERT

ARCHITECTURE DIAGRAM



DESCRIPTION : In the **EXISTING SYSTEM**, Door Lock status is verified manually there is no automatic process is implemented. In the **PROPOSED SYSTEM**, we have developed a security system that interfaces with an Android mobile device. The mobile device and security system communicate via GPRS. The mobile application can be loaded onto any compatible device, and once loaded, interface with the security system. Commands to lock, unlock, or check the status of the door to which the security system is installed can be sent quickly from the mobile device via a simple, easy to use GUI. The **MODIFICATION** that we propose, is IR sensor is attached in the door, if any person is detected an automatic Alert SMS is send to the User's Mobile, so that user can initiate the webcam and can see the Images of the persons who are waiting via their mobile through GPRS Communication. Mobile User can open the Door to the known persons by sending a Authenticating Key to the server.

DOMAIN: Mobile Computing, Security, Embedded, Android

DNAP 1014. (J2EAP 11021). ANDROID IMPLEMENTATION FOR DISCOUNT AND LOYALITY COUPONS WITH SECURITY SYSTEM

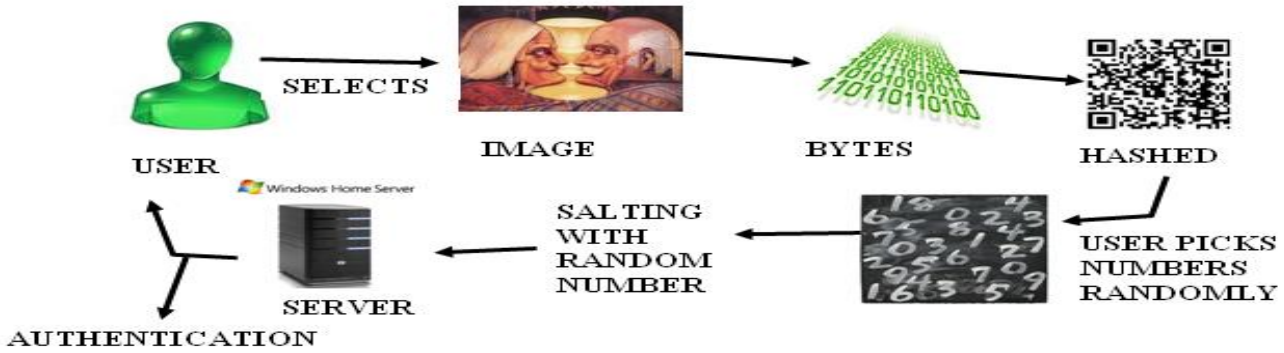
ARCHITECTURE DIAGRAM

DESCRIPTION : In the **EXISTING SYSTEM,** we're purchasing the products via online (Over internet from the users PCs). Though online retailing is featured in mobile, that wasn't developed as much as compared to the retailing via PCs and Laptops. In the **PROPOSED SYSTEM,** We can purchase the products through our Android Smartphone. The user will hit the shopping server from their Android mobile with NFC Tag. The once they've entered into the site, they can purchase the items. Here we're providing the NFC ID to each and every user so that they enter it whenever they're signing into the site. In the **MODIFICATION**, we're sending an SMS alert to the user's mobile phone regarding the "deals of the day". This lets the users to know the deals, so that they can purchase the products. Also we're writing the Image Coupon Id in the NFC tag. This ensures the security for the users.

DOMAIN: Mobile Computing, Security, Embedded, Android

DNAP 1015. (J2EAP 11023). IMAGE BASED SECURED PASSWORD AUTHENTICATION SCHEME USING HASHED BYTES WITH SALTING PROCESS

ARCHITECTURE DIAGRAM

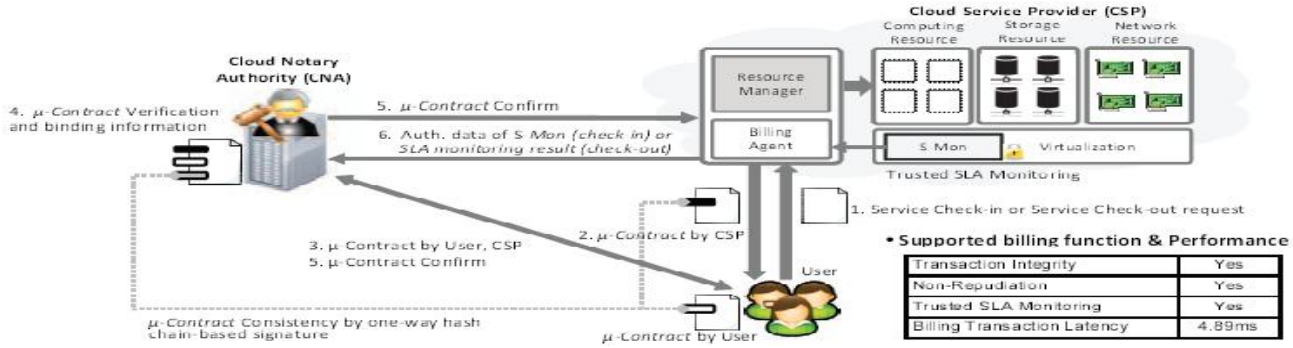


DESCRIPTION : In the **EXISTING SYSTEM**, Password Schemes intended to deploy or encourage the use of Strong Passwords have failed. So in the **PROPOSED MODEL**, Object-Based Password (Obpwd) is introduced in which user Selects a Image/ Text/ Video Which is Converted into Bytes. This Bytes are Encrypted by RSA Algorithm, Then Made Hash. Out of this long Hash Data user Provides of the Part of the Data which is compared then Authenticated. The **MODIFICATION** that we Propose is Salting which is added by the User with the User's input of Hash Data. The Same Input Hash Data is not accepted again by the Server Unless Second Cycle Starts.

DOMAIN: Security

DNAP 1016. (J2EAP 11024). THEMIS: A MUTUALLY VERIFIABLE BILLING SYSTEM FOR THE CLOUD COMPUTING ENVIRONMENT

ARCHITECTURE DIAGRAM

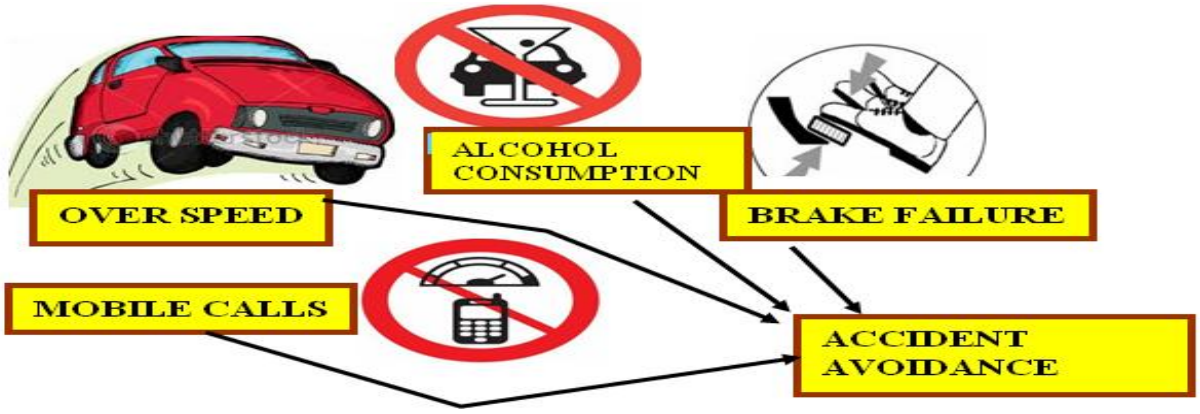


DESCRIPTION : With the widespread adoption of cloud computing, the ability to record and account for the usage of cloud resources in a credible and verifiable way has become critical for cloud service providers and users alike. The success of such a billing system depends on several factors: the billing transactions must have integrity and non repudiation capabilities; the billing transactions must be non obstructive and have a minimal computation cost; and the service level agreement (SLA) monitoring should be provided in a trusted manner. Existing billing systems are limited in terms of security capabilities or computational overhead. In this paper, we propose a secure and non obstructive billing system called THEMIS as a remedy for these limitations. The system uses a novel concept of a cloud notary authority for the supervision of billing. The cloud notary authority generates mutually verifiable binding information that can be used to resolve future disputes between a user and a cloud service provider in a computationally efficient way.

DOMAIN: Cloud Computing, Security

DNAP 1017. (J2EAP 11025). PROACTIVE ACCIDENT AVOIDANCE SYSTEM USING DRIVER AND VEHICLE BEHAVIOURAL ANALYSIS PATTERN

ARCHITECTURE DIAGRAM

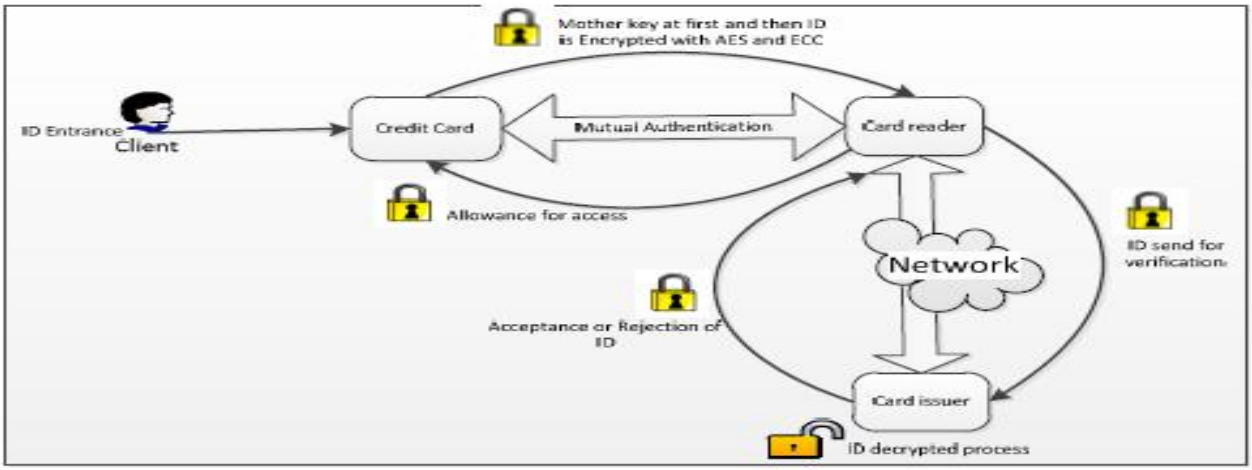


DESCRIPTION : In this paper, a novel accident Avoidance system for the identification of the main human factors involved on traffic accidents is presented. In this system, of implementation, we are Proposing, Dynamic Accident Avoidance System. We include Alcohol Sensor to identify the Driver's Alcohol Consuming status along with Mobile Calls monitoring system to automatic Braking System to control the Speed of the Vehicle when the Drier gets the Calls. We also include Speed control Mechanism to avoid Accidents due to Over Speed.

DOMAIN: Mobile Computing, Embedded

DNAP 1018. (J2EAP 11026). NFC BASED SECURED MULTIPURPOSE SMART CARD SYSTEM FOR COMMON PUBLIC UTILITY

ARCHITECTURE DIAGRAM



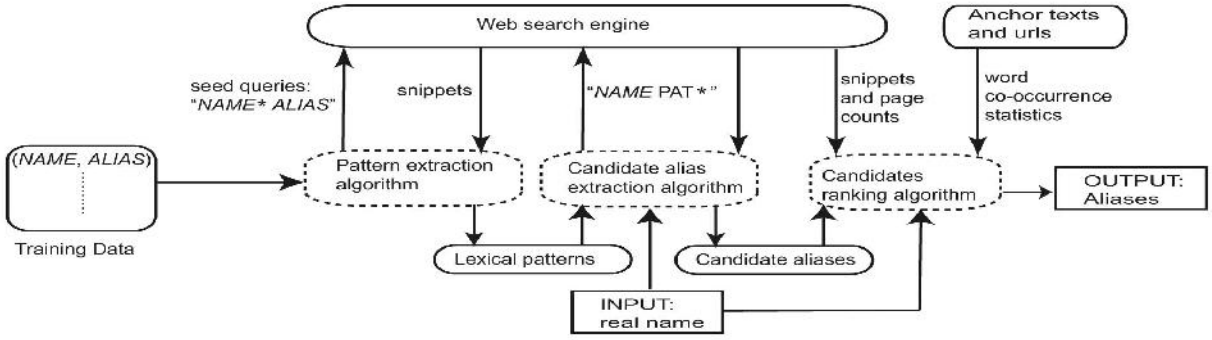
DESCRIPTION : Smart cards have many applications such as health, ID verification and access control, electronic purse card, banking card, payphone card, passport card and license card. Since, there are many kinds of smart cards, it is difficult to carry and protect them. Losing one card means losing a lot of important information. So in this paper proposes to combine some important cards such as: health, passport and credit system in one multipurpose smart card and find an encryption method to make it enough secure. It should also be efficient in transferring

information. It means, we develop an effective encryption system for these three applications in a multipurpose smart card and we propose an optimized encryption system for the applications.

DOMAIN: Mobile Computing, Security, Embedded

DNAP 1019. (J2EAP 11027). PATTERN BASED EXTRACTION SYSTEM OF AUTONOMOUS DISCOVERY OF PERSONAL NAME AND ALIASES FOR EFFECTIVE INFORMATION REDRIVES

ARCHITECTURE DIAGRAM



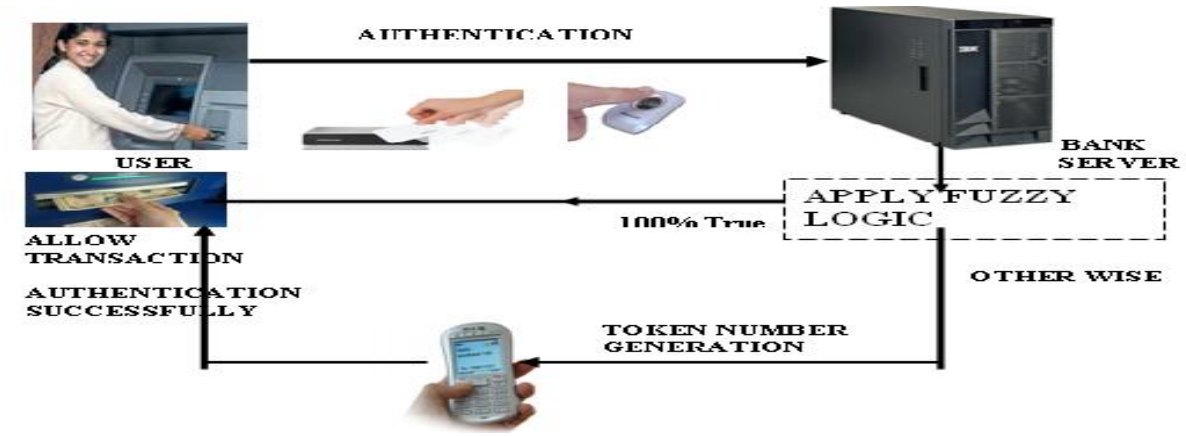
DESCRIPTION : In the **EXISTING SYSTEM**, An individual is typically referred by numerous name aliases on the web. Accurate identification of aliases of a given person name is useful in various web related tasks such as information retrieval, sentiment analysis, personal name disambiguation, and relation extraction. We **PROPOSE** a method to extract aliases of a given Personal Name from the Web. Given a Personal name, the Proposed Method first Extracts a set of Candidate Aliases. Second, we rank the extracted candidates according to the likelihood

of a candidate being a correct alias of the given name. We propose a novel, automatically extracted lexical pattern-based approach to efficiently extract a large set of candidate aliases from snippets retrieved from a web search engine. Our **MODIFIED IMPLEMENTATION** Verifies the Profession / Job carried by the Name and Aliases. Because in few cases there may be more People with same Name & Aliases but the Profession would differ. This Process definitely a Best Method to Identify Name and the Aliases of any user.

DOMAIN: Data Mining

DNAP 1020. (J2EAP 11029). FUZZY IMPLEMENTATION OF BIOMETRICS WITH FIVE FACTOR AUTHENTICATION SYSTEM FOR SECURED BANKING

ARCHITECTURE DIAGRAM



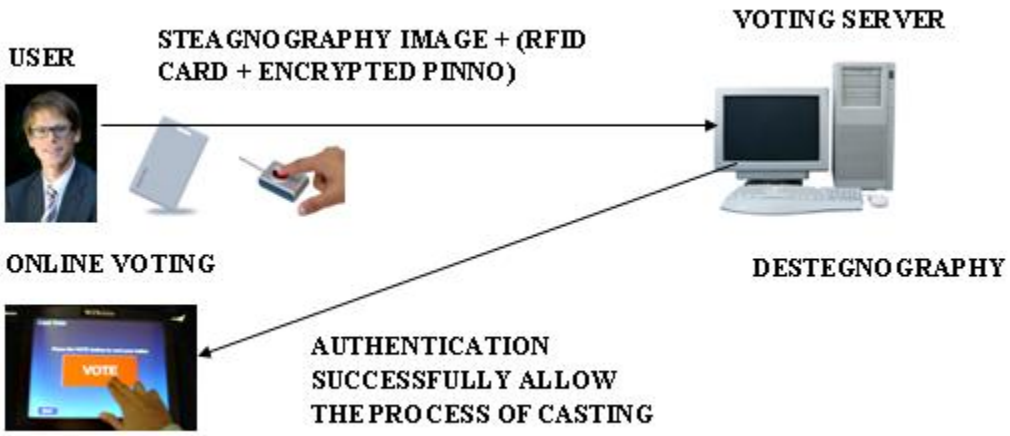
DESCRIPTION : In the **EXISTING SYSTEM**, any one of the Authentication Procedures are Process, like Finger Print, RFID card, PIN. In the **PROPOSED MODEL** all those are used together for authentication. For Finger print Fuzzy Logic is applied for Exact

Mapping and Proper Authentication. In the **MODIFICATION** Process, if finger print's fuzzy rule says 60 – 80% of matching then One Time Password (OTP) is Generated as SMS to the User's Mobile. User will be giving OTP via Keypad Matrix. Along with the OTP, Key Pad ID is also passed for authentication. If Fingerprint, RFID card, PIN and OTP, Keypad ID (If Fingerprint is 60-80% matched) which become five factor authentication.

DOMAIN: Security, Mobile Computing, Embedded

DNAP 1021. (J2EAP 11030). SECURED ONLINE VOTING SYSTEM WITH STENOGRAPHY IMPLEMENTATION USING RFID & FINGER PRINT TECHONOLOGY

ARCHITECTURE DIAGRAM



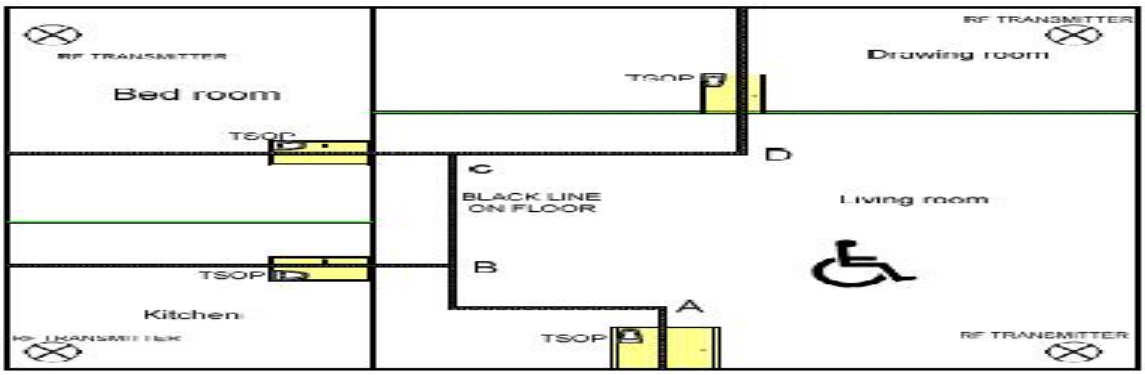
DESCRIPTION : In the **EXISTING SYSTEM**, Online Voting is used to Cast their Votes which has no significant security. In the **PROPOSED MODEL**, Steganography is

introduced. Steganography is Hiding Text in a Image. User will be Providing Finger Print, RFID (smart) Card and PIN Number. PIN is Encrypted using RSA, then RFID card number and encrypted Pin number is made Steganographed with user's Finger Print Image then sent to the Voting Server. The Voting Server will Destegano and also Decrypt PIN to get Original Finger Print Image, RFID and PIN Number and verified with the User's Registration Details. If authenticated Success Voting is Permitted. The **MODIFICATION** is, user can also check the Party to which Vote of his has been Casted really.

DOMAIN: Mobile Computing, Security

DNAP 1022. (J2EAP 11033). DYNAMIC AND AUTOMATED VOICE BASED CONTROL OF WHEEL CHAIR FOR PHYSICALLY CHALLENGED PEOPLE

ARCHITECTURE DIAGRAM

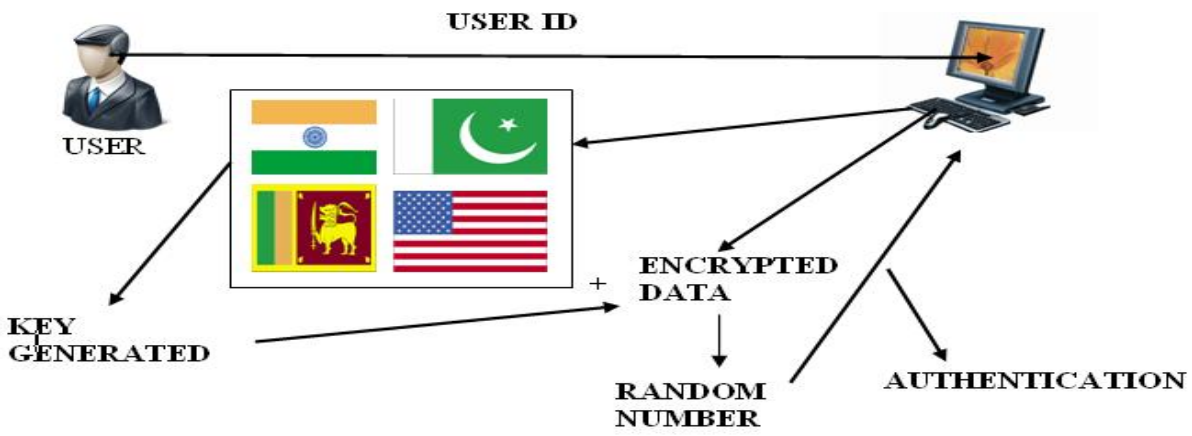


DESCRIPTION : In the **EXISTING SYSTEM**, the elderly (or) physically handicapped people will have to depend on others for the movement of wheel chair. In the **PROPOSED MODEL**, Intelligent Home Navigation System (IHNS) which comprises of a wheelchair, voice module and navigation module. By making use of IHNS, elderly and the physically challenged can go to different rooms in the house like kitchen, living room, dining room etc by just speaking a word which is predefined to that particular room. Voice of the person is captured compared using speech recognition to detect the place to which person has to move. Each door of the room is deployed with IR value and once Voice is Recognized the Wheel Chair starts to move, it is automatically stopped until Desired IR value is obtained. The **MODIFICATION** is that wheel chair would be provided with emergency button of the patients health is not control stage and immediate alert is passed as SMS to the doctor.

DOMAIN: Mobile Computing, Embedded

DNAP 1023. (J2EAP 11034). SECURED & IMPLICIT PASSWORD AUTHENTICATION TO AVOID SHOULD SURFING ATTACK

ARCHITECTURE DIAGRAM

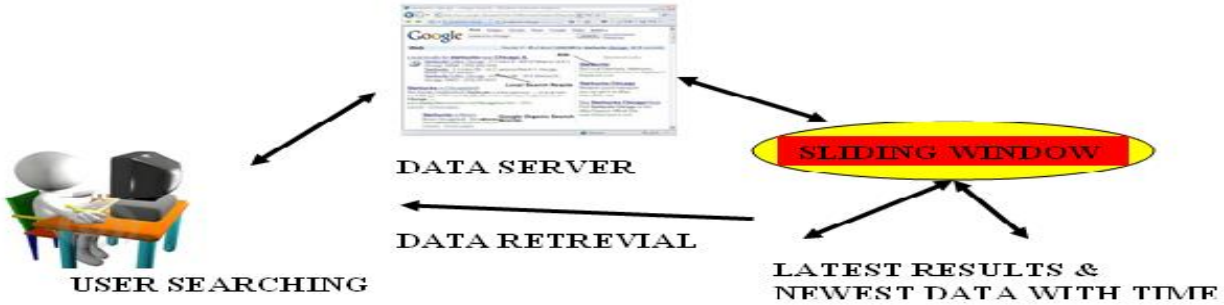


DESCRIPTION: In the **EXISTING SYSTEM**, user enters the password manually, so there is lot of process of shoulder surfing attacks. In order to avoid this **PROPOSED SYSTEM**, is used, in which user has to enter the user ID then the Server Provides with Encrypted Data and set of Images. These Images are the Implicit Answers for the Questions asked to that user during Registration process. If the user clicks on the Correct Image then key is given to the User. User Provides the key on to the Encrypted Data, Original Data appears. Original data is verified by the Main Server for Authentication. The **MODIFICATION** proposed, is the Sending of the key as SMS to the User's Mobile if Correct Image is selected. So we are verifying User ID, Correct Image, User's Mobile Number and the Original Data which ensures Perfect Security.

DOMAIN: Security, Mobile Computing

DNAP 1024. (J2EAP 11035). EFFICIENT AND EFFICIENT UPDATED DATA RETRIEVAL SYSTEM CONTINUOUS TEXT SEARCH QUERIES

ARCHITECTURE DIAGRAM



DESCRIPTION : Consider a text filtering server that monitors a stream of incoming documents for a set of users, who register their interests in the form of continuous text search queries. The task of the server is to constantly maintain for each query a ranked result list, comprising the recent documents (drawn from a sliding window) with the highest similarity to the query. Such a system underlies many text monitoring applications that need to cope with heavy document traffic, such as news and email monitoring. In this paper, we propose the first solution for processing continuous text queries efficiently. Our objective is to support a large number of user queries while sustaining high document arrival rates. Our solution indexes the streamed documents in main memory with a structure based on the principles of the inverted file, and processes document arrival and expiration events with an incremental threshold-based method.

DOMAIN: Data Mining

DNAP 1025. (J2EAP 11037). DATA INTEGRITY AND SECURITY SYSTEM USING ENCRYPTION IN CLOUD COMPUTING PROCESS

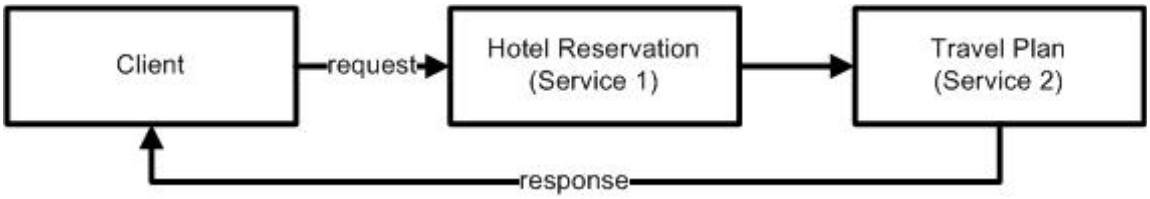
ARCHITECTURE DIAGRAM

DESCRIPTION : In the **EXISTING SYSTEM**, security is the major issue to be discussed in the Cloud Computing process. Internet threats are increased so data security is to be discussed is to be maintained. In the **PROPOSED MODEL**, the Data stored in a Cloud Server is split into blocks. The Integrity of the blocks are verified randomly by the Third Party Verifier. Verifier will give its public key then the Challenge to a particular Block. The Block will respond with Challenge Response. The Verifier verifies the CR, if it is Genuine then the data is safe condition; if not data Access is blocked. In the **MODIFICATION PROCESS**, the verifier will be given the public key then encrypted password, Challenge & Challenge Response are Encrypted using RSA. The Entire data is also encrypted. This Process ensures Security in Cloud computing.

DOMAIN: Data Mining, Security, Cloud Computing

DNAP 1026. (J2EAP 11039). AUTOMATIC COMPUTATION SYSTEM FOR COMPOSED WEB SERVICES USING INTER LINKED USER BEHAVIOUR

ARCHITECTURE DIAGRAM

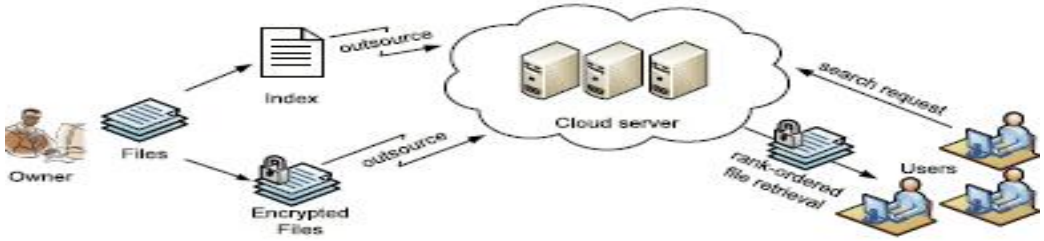


DESCRIPTION : In the **EXISTING SYSTEM**, the Process are Compute Manually. User shloud Proceed Manually. In the **PROPOSED SYSTEM**, Automatic Computing with Web Services is executed. Services are Deployed in Cloud. This project dynamically initiates the other related services from Cloud by Observing the User next Interest based on the Previous. The **MODIFICATION** is to get the feedback from the Previous Users, and Highly Ranked Service Provider is Promoted first to the User from Web Service and Cloud.

DOMAIN: Cloud Computing, Web Services

DNAP 1027. (J2EAP 11041). DEVELOPMENT OF SECURED KEY WORD SEARCH AND RETRIEVAL OF BEST RANKED ENCRYPTED DATA IN CLOUD ENVIRONMENT

ARCHITECTURE DIAGRAM

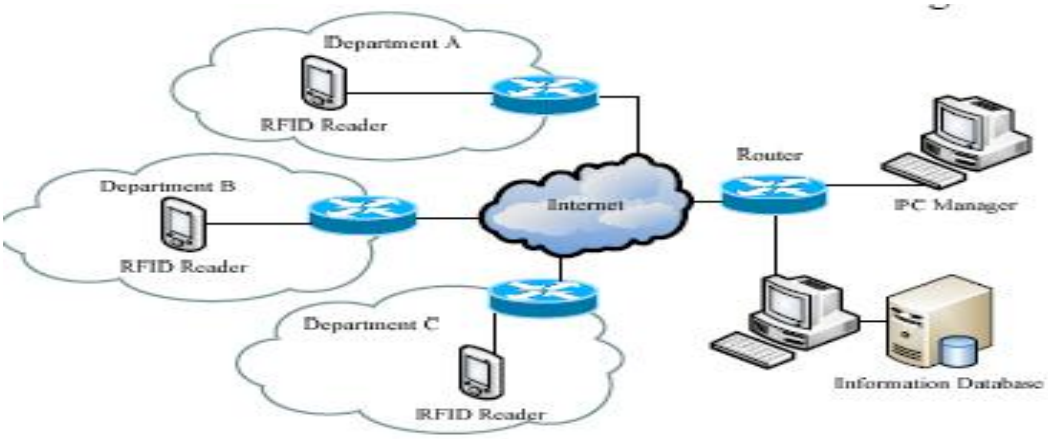


DESCRIPTION : Cloud computing economically enables the paradigm of data service outsourcing. However, to protect data privacy, sensitive cloud data have to be encrypted before outsourced to the commercial public cloud, which makes effective data utilization service a very challenging task. Although traditional searchable encryption techniques allow users to securely search over encrypted data through keywords, they support only Boolean search and are not yet sufficient to meet the effective data utilization need that is inherently demanded by large number of users and huge amount of data files in cloud. In this paper, we define and solve the problem of secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by enabling search result relevance ranking instead of sending undifferentiated results, and further ensures the file retrieval accuracy. Specifically, we explore the statistical measure approach, i.e., relevance score, from information retrieval to build a secure searchable index, and develop a one-to-many order-preserving mapping technique to properly protect those sensitive score information. The resulting design is able to facilitate efficient server-side ranking without losing keyword privacy.

DOMAIN: Cloud Computing, Security, Data Mining

DNAP 1028. (J2EAP 11042). NFC AND BIOMETRICS IMPLEMENTATION FOR EFFECTIVE EMPLOYEE MANAGEMENT SYSTEM WITH SMS ALERT

ARCHITECTURE DIAGRAM

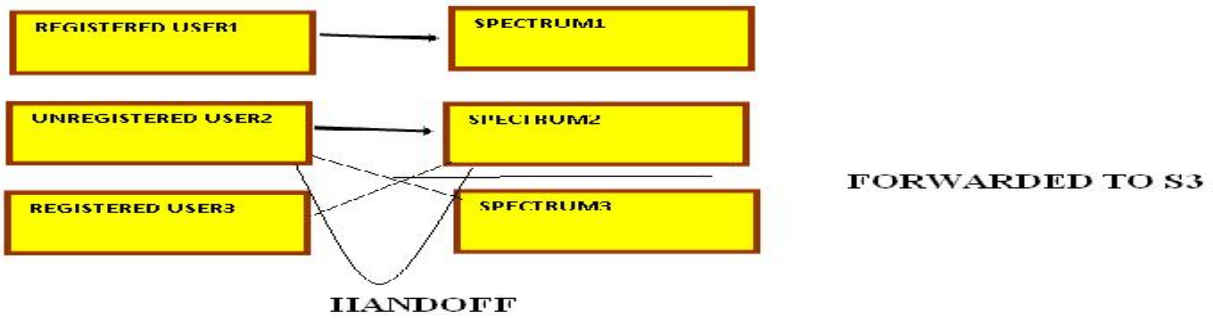


DESCRIPTION : In the **EXISTING SYSTEM**, the Educational Institutions would send the Attendance Records manually to the Parents (or) through Monthly Alert as SMS. In the **PROPOSED SYSTEM**, the student's presence would be send as SMS to the Parents immediately that day itself on a Daily Basis. Every Student would be provided with Finger Print Authentication. The **MODIFICATION** that we propose is RFID card is provided to every User as ID Card. RFID Card and Finger print is matched only then Attendance is recorded and SMS Alert is send to the Parents.

DOMAIN: **Mobile Computing, Embedded**

DNAP 1029. (J2EAP 11043). AUTONOMOUS SPECTRUM HANDOFF FRAMEWORK IN ADHOC NETWORK WITH DYNAMIC LOAD BALANCING

ARCHITECTURE DIAGRAM

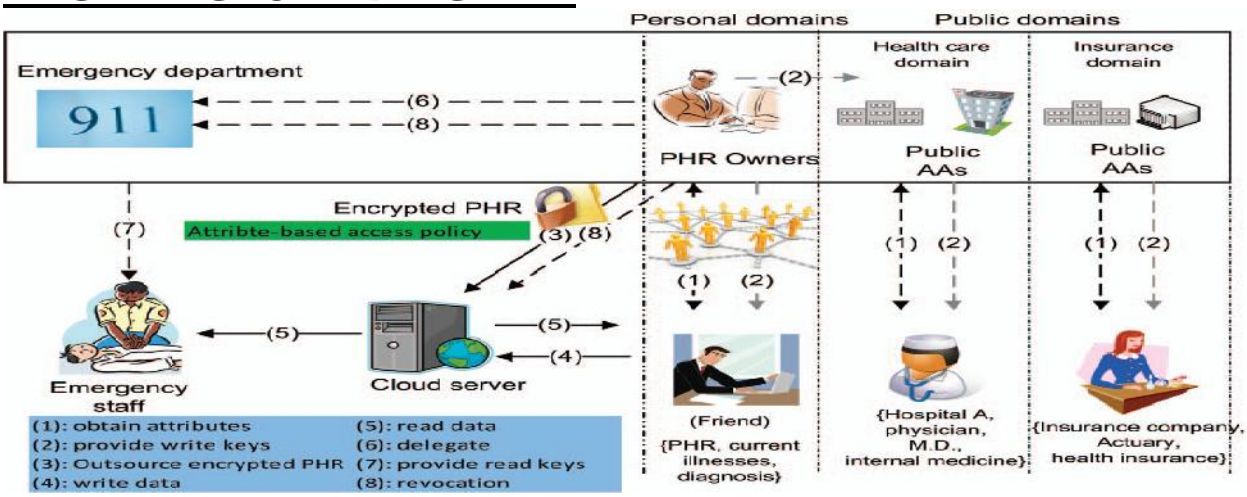


DESCRIPTION : In the **EXISTING SYSTEM**, Although the Cognitive Radio (CR) technology is a promising solution to enhance the spectrum, only it provides sufficient support to the licensed users or primary users and not to the Unlicensed Users. In the **PROPOSED MODEL**, a proactive spectrum handoff framework for CR ad hoc networks, ProSpect, is proposed to address these concerns. In the proposed framework, Channel-Switching (CW) policies and a proactive spectrum handoff protocol are proposed to let unlicensed users vacate a channel before a licensed user utilizes it to avoid unwanted interference. Network coordination schemes for unlicensed users are also incorporated into the spectrum handoff protocol design. In the **MODIFICATION** that we propose is a unlicensed user is handled by the spectrum and receives the request from the licensed user, the system automatically transfer the unlicensed user into another spectrum which reduces load and the waiting time for particular unlicensed user.

DOMAIN:. **Mobile Computing**

DNAP 1030. (J2EAP 11044). DESIGN OF EFFECTIVE ATTRIBUTE BASED ENCRYPTED SECURITY SYSTEM FOR PUBLIC AND PERSONAL CLOUD COMPUTING SYSTEM

ARCHITECTURE DIAGRAM



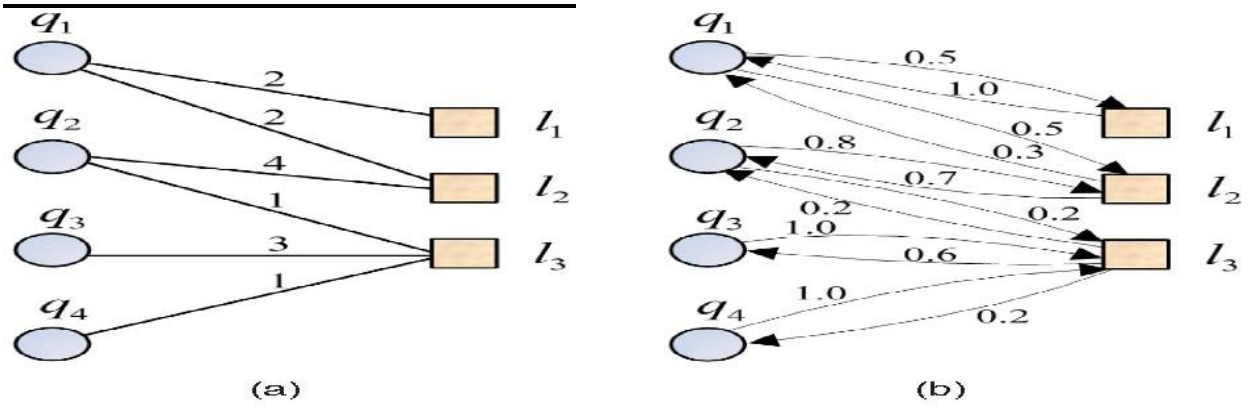
DESCRIPTION : In the **EXISTING SYSTEM**, Personal health record (PHR) is an emerging patient-centric in Cloud Computing Servers. However, there is no Security in keeping privacy concerns of the Patient & could be exposed to those third party servers and to unauthorized parties. In the **PROPOSED MODEL**, 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.
[2]

DOMAIN: Cloud Computing, Security

DNAP 1031. (J2EAP 11046). GENERALISED AND PERSONALISED WEB SEARCH WITH FEEDBACK BASED RE - RANKING SYSTEM

ARCHITECTURE DIAGRAM



DESCRIPTION : In the **EXISTING SYSTEM**, Innumerable different kinds of recommendations are made on the Web every day, including movies, music, images, books recommendations, query suggestions, tags recommendations, etc. No matter what types of data sources are used for the recommendations, essentially these data sources can be modeled in the form of various types of graphs. In the **PROPOSED SYSTEM**, there are three methods to be adopted. 1. Diffusion directed 2. Diffusion Undirected. 3. Random Jump. In the **MODIFICATION** process, we get the feedback from the users and then the corresponding server will Re-rank the data and provided to the new user.

DOMAIN: Data Mining

DNAP 1032. (J2EAP 11047). MULTI INPUT DEVICE CONTROL WITH VIBRATION DETECTION IN CLOUD COMPUTING USING ANDROID

ARCHITECTURE DIAGRAM

DESCRIPTION : In the **EXISTING SYSTEM**, very few Device Control process is Wireless and most of our home Appliances control is via Wired Connection. If at all there is wireless communication has its own range. Control of Devices is achieved in a Short Range only. In the **PROPOSED SYSTEM,** we have developed a Home Automation system that employs the integration of multi-touch mobile devices, cloud networking, wireless communication, and remote control of various lights and appliances within their home. This system uses a consolidation of a mobile phone application, handheld wireless remote, and PC

based program to provide a means of user interface to the consumer. The **MODIFICATION** that we propose is Vibration Sensor is connected to the User PC, if the Vibration is detected Automatic Alert SMS is send to the mobile number of Authorized Person.

DOMAIN: Mobile Computing, Embedded, Android

DNAP 1033. (J2EAP 11048). AUTOMATIC DATA MINING TECHNIQUE FOR PREDICTING SALES PERFORMANCE ON A PRODUCT QUALITY DOMAIN

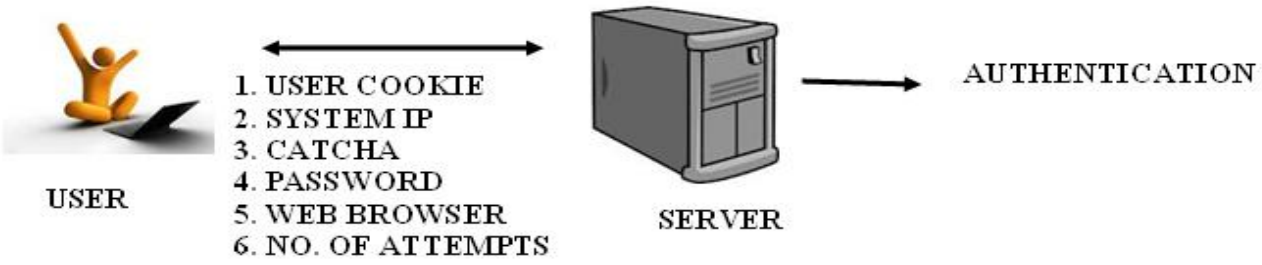
ARCHITECTURE DIAGRAM

DESCRIPTION : In the **EXITING SYSTEM**, posting online reviews has become a common practice for e-commerce websites to provide the venues and facilities for people to publish their reviews. Prior studies of product sales failing to consider the effect of the sentiments present in the blogs and strong correlation between the volume of reviews and sales spikes, using the volume or the link structures alone do not provide satisfactory prediction performance. In the **PROPOSED SYSTEM**, we are implementing this process for product purchase. The manufacturer initially gives their feedback process to the main server, and then the main server will Re-rank according to the quality which displayed to the new user's. The server will update auto regressive process to find out the product category. We apply S-PLSA algorithm to predict the performance of the product. In the **MODIFICATION** phase, user can make a query to the server specifying a general product. The server will predict the best product with the best deals by comparing the rest of the relevant and the manufacturers.

DOMAIN: Data Mining

DNAP 1034. (J2EAP 11051). PREVENTION OF ONLINE PASSWORD HACKING PROCESS WITH SECURED MULTI AUTHENTICATION SCHEME

ARCHITECTURE DIAGRAM



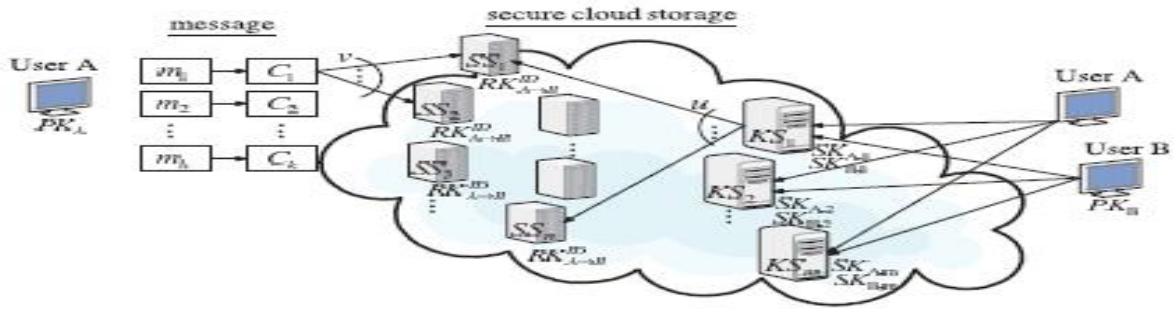
DESCRIPTION : In the **EXISTING MODEL**, online Guessing attacks on Password Based Systems are inevitable and commonly observed against Web Applications. In the **PROPOSED SYSTEM**, the Server Verifies (1) User Name from the Cookie of the User's Machine, (2) System IP, (3) Capcha, (4) Password of the 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.

DOMAIN: Network Security

DNAP 1035. (J2EAP 11052). DISTRIBUTION OF SECRET KEYS AND THE PACKETS FOR SECURED DATA FORWARDING SCHEME IN CLOUD SERVER

ARCHITECTURE DIAGRAM



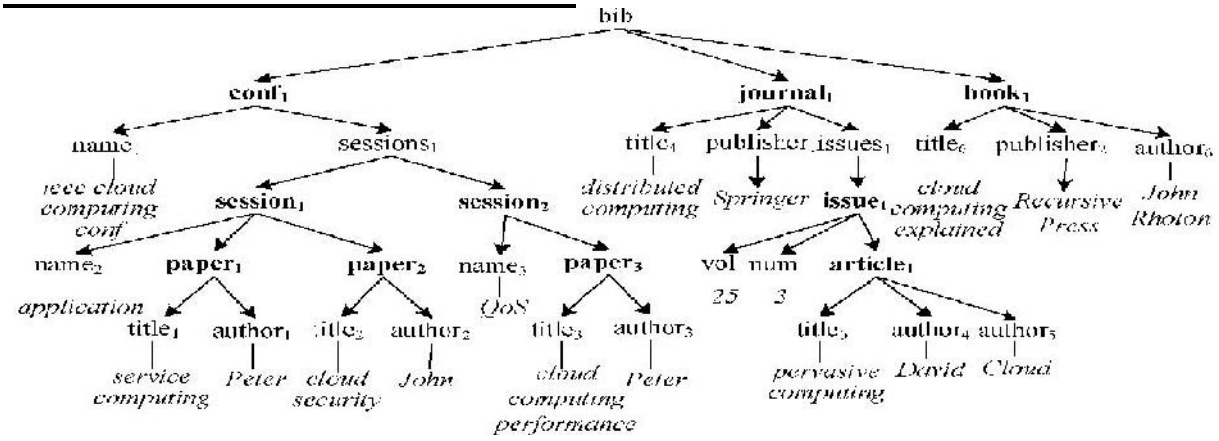
DESCRIPTION : In the **EXISTING SYSTEM**, Cloud Computing is the Process of Storing the Data in the Remote Server. This Process Doesn't Speak about Confidentiality of the Data. So in the **PROPOSED MODEL**, the Uploaded file from a Data Owner is Splitted into Multiple Packets and Stored in Multiple Cloud Servers. These Packets are Encrypted Using the Primary Key. These Different Keys are also distributed in Multiple Key Servers. User ID is

Appended for Verification. If the Data Owner Forwards the file then the Keys are Verified for the Data Access. The **MODIFICATION** that we Propose is the Sending the Secret Key as SMS to the Shared / Forwarded Nodes for the Process of Proper Security.

DOMAIN: Cloud Computing, Security

DNAP 1037. (J2EAP 11055). DEVELOPMENT OF XML BASED KEYWORD SEARCH WITH CLUSTERED RESULTS FOR EFFECTIVE & SPEEDY DATA RETRIEVAL

ARCHITECTURE DIAGRAM



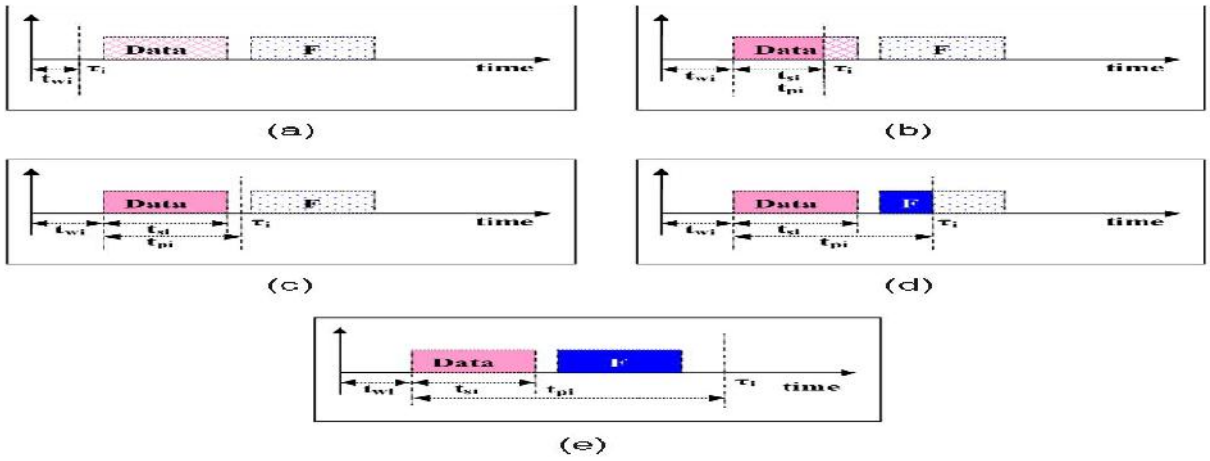
DESCRIPTION : In the **EXISTING SYSTEM**, Google Search is the Prevailing one which Retrieves the Resultant Pages with Respect to the Number of Hit Proportion of Users. In

the **PROPOSED MODEL** XML Based Search is Made Practically with Clustering of Results. Active Search Process is implemented. Rather Showing the Results One by One, we aim to Group / Cluster the Results, So that User Selects the Group if Interested Which would Reduce the Result Categories. The **MODIFICATION** that We Propose is Data Owner can Upload the Documents from any Database Format So that it is Converted into XML Format.

DOMAIN: Data Mining

DNAP 1038. (J2EAP 11057). ADAPTIVE LOCATION BASED CONTENT DELIVERY USING ACCESS POINT CENTRIC AND DEPUTY & FORWARD MECHANISM

ARCHITECTURE DIAGRAM

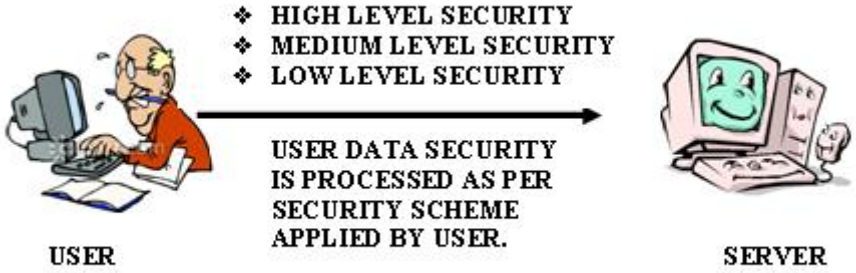


DESCRIPTION : In the **EXISTING SYSTEM**, we introduce a delay-sensitive service that involves transmitting large amounts of location-based data to nodes at multiple locations. Given a limited amount of access points (AP) and an abundance of service requests that result from the nodes moving around, a typical content delivery service would inevitably introduce considerable delay. In the **PROPOSED MODEL** both AP Centric and Deputy & Forward Model is introduced. If the Transactions are made by AP then it is called as AP Centric. If Node 1 has got a Data through AP, Node 2 request for the same Data then AP will Depute Node 1 to Forward the Data to Node 2 if Node 1 is within the control of that AP. The **MODIFICATIONS** that we Propose is Node 1 will Transfer the Data to Node 2 until Node 1 leaves that Area (AP) , then AP will continue the Data Transfer automatically.

DOMAIN: Mobile Computing

DNAP 1039. (J2EAP 11058). SECURED IAAS IMPLEMENTATION OF CLOUD COMPUTING WITH MULTILEVEL INTRUSION DETECTION SYSTEM WITH SMS ALERT

ARCHITECTURE DIAGRAM

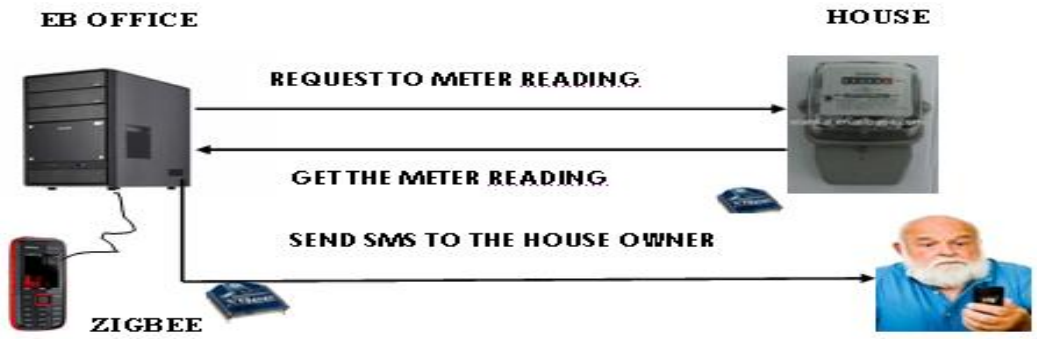


DESCRIPTION : In the **EXISTING SYSTEM**, Cloud Computing is a new type of service which provides large scale computing resource to each customer. Cloud Computing systems can be easily threatened by various cyber attacks, because most of Cloud Computing systems provide services to so many people who are not proven to be trustworthy. In the **PROPOSED MODEL** of implementation three levels of Cloud Process are implemented i.e., High, Medium and Low Levels of Security. High level implementation contains all sorts of security like IP Address, Malicious Code checking, and Request Acceptance, Time of Request, Password and others. Medium Level Process is bit low verification factors when compared to High Level. Low level very less authentication these verification would ensure security in cloud computing. The **MODIFICATION** that propose is generating a as session key using MD5 algorithm to the user's mobile which would dynamically change very time.

DOMAIN: Cloud Computing, Security

DNAP 1040. (J2EAP 11059). REMOTE AND INTELLIGENT AUTOMATIC METER READING (AMR) WITH COST AS SMS ALERT AND AUTOMATIC PAYMENT SYSTEM USING ZIGBEE

ARCHITECTURE DIAGRAM

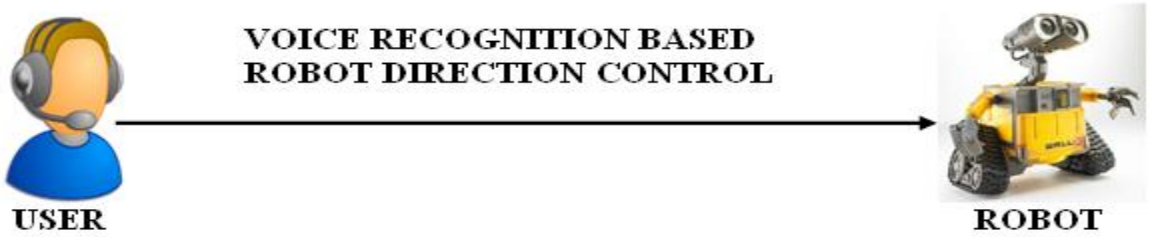


DESCRIPTION : In the **EXISTING SYSTEM**, EB Persons would come to the house manually for calculating the EB Charges. In the **PROPOSED MODEL**, the Automatic process of fetching the EB charges is proposed. EB server is connected with zigbee sends request to Every Home for the Automatic EB Meter Readings (AMR). Every house is connected with the zigbee which in return transmits the value back to the EB server with user ID. The values are updated in the EB Server. The **MODIFICATION** is automatic alert SMS of cost is send to the customers. The Amount is automatically detected from the Bank Account of the Customer.

DOMAIN: Mobile Computing, Embedded

DNAP 1041. (J2EAP 11062). VOICE BASED NAVIGATION CONTROL OF WIRELESS REMOTE USING RF TECHNOLOGY

ARCHITECTURE DIAGRAM



DESCRIPTION : In the **EXISTING SYSTEM**, the Robot control is carried using Manual way. In the **PROPOSED MODEL**, admin can control the Robot using voice based navigation. User's Voice has to be matched using Speech Recognition process by comparing with previously Trained Voice of the User. **MODIFICATION** we propose is the Robot can be controlled using Remote system as well as Remote Java Mobile through GPRS communication.

DOMAIN: Mobile Computing, Embedded

YOUR OWN IDEAS ALSO