ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. IV, Issue IV, April 2018

DOCTORS COMMUNE

V. Srinivasan[1], T.S. Sudarshan[2], S. Narendran[3], R. Sashwath Prasad[4], R. Rengaraj alias muralidharan[5]
Department of Information Technology, saranathan college , Trichy, India[1,2,3,4]
Assistant Professor, Saranathan College of Engineering, Trichy,India[5]

***Abstract*—The use of information technology and management systems for the betterment of health care is more important and popular. However, existing efforts mainly focus on information of hospitals or medical institutions within the organizations, and few are directly oriented to the patients, their families, and other ordinary people. The main importance of this website is to improvise the interaction between the doctors and general public. Another highlight of this project is that each and every user is thoroughly verified to the core and the access is given with the reliable contents. No BOGUS doctors can enter in this system as the ADMIN of the site continuously authenticates the activities.**

***Index Terms*: health care, appointment, authentic doctor**

I)INTRODUCTION

The contradiction between per-capita level of medical resources and the growing demand from people for health care is increasing. Thus, how can we best utilize the limited medical resources to provide more efficient health care services for people and to construct new medical service systems becomes a serious and urgent problem. The problems faced in the field of medical and health care such as the aging of the population, the increase of chronic patients, the rising medical expenses, and the needs to improve the quality of medical services are common around the world today. In order to solve them, information technology (IT) must be deployed to this field. In recent years, medical information systems play an increasingly important role in supporting doctors and nurses, enhancing the quality of medical services, reducing the medical expenses, and improving the care of chronic patients. Therefore, medical informatization has drawn more and more attention in various countries. The main objective of this website is to improvise the interaction between the doctors and general public. Another highlight of this project is that each and every user is thoroughly verified to the core and the access is given with the reliable contents. No BOGUS doctors can enter in this system as the ADMIN of the site continuously authenticates the activities.

In the early 1960s, the U.S. began the study of hospital information system (HIS). In 1985, according to a survey of them used computers to manage the finance charge, and 25% of them had relatively integrated HIS. By the year 2004, 20% of the hospitals in the U.S. had completed electronic medical record (EMR) system transformation and picture archiving and communication system (PACS) experimentation. The National Committee on Vital and Health Statistics of the U.S. submitted a strategic report "*Information for Health: A Strategy for Building the National Health Information Infrastructure (NHII)* to the congress in 2001, which introduced the planningblueprint of establishment of the national health informationinfrastructure from three aspects: personal health, medical institution, and public health.

Often health system has been defined with a reductionist perspective, for example reducing it to healthcare system. In many publications, for example, both expressions are used interchangeably. Some authors have developed arguments to expand the concept of health systems, indicating additional dimensions that should be considered:

Health systems should not be expressed in terms of their component only, but also of their interrelationships; Health systems should include not only the institutional or supply side of the health system, but also the population Health systems must be seen in terms of their goals, which include not only health improvement, but also equity, responsiveness to legitimate expectations, respect of dignity, and fair financing, among others;

Health systems must also be defined in terms of their functions, including the direct provision of services, whether they are medical or public health services, but also "other enabling functions, such as stewardship, financing, and resource generation, including what is probably the most complex of all challenges, the health workforce."

II)LITERATURE SURVEY

I) Adaptive service composition in flexible processes

D. Ardagna and et.alproposed an Experimental results compare our method with other solutions proposed in the literature and demonstrate the effectiveness of our approach toward the identification of an optimal solution to the QoS constrained Web service selection problem. In service-oriented environments, complex applications can be described as processes invoking services selected at runtime. In this scenario, applications are defined as flexible processes composed of abstract Web services. Web services are selected from a set of functionally equivalent services, that is,

All Rights Reserved © 2018 IJARMATE

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. IV, Issue IV, April 2018

services which implement the same functionality but differ for nonfunctional characteristics, i.e., Quality of Service (QoS) parameters. The goal is to select the best set of services available at runtime, taking into consideration process constraints, but also end-user preferences and the execution context.The Web service selection problem has been studied for business processes and e-science. Dynamic Web service selection for composed Web services focused in particular on context aware business processes. Context awareness may be needed both when considering Web service personalization, where a generic process is personalized choosing services according to user preferences, and in mobile composed services, to provide ubiquitous services where selection and execution depend on the available services and their QoS.

II) Knowledge-based programming: A survey of program design and construction techniques

Goldberg and et.aldiscussion is the notion of program development by means ofprogram transformation. Using this methodology, a formal specification is compiled (either manually or automatically) into an efficient implementation by the repeated application of correctness-preserving, source-to-source transformations. Software development is a knowledge-intensive activity. A promising approach to improving the efficiency of software development is the construction of a knowledge-based software assistant. Such a system provides the medium of interaction for the development process and enforces the semantic consistency of the program as it evolves from its specification to its implementation. A system that provides automated assistance for program development can do so to the extent to which it embodies knowledge of the programming process and knowledge of the application domain for which the program is written. Programmers have knowledge of how to represent problem-domain objects with the data structure facilities of their programming language, how to implement various search techniques and other programming clichés, the efficiency of various program constructions, and so on. This paper surveys our understanding and formalization of this knowledge. It is presented from the point of view of algorithm design and high-level program optimization. It discusses techniques for data structure selection, the procedural representation of logic assertions, store-versus-compute, finite differencing, loop fusion, and algorithm design methods.

III)Wrapping Client-Server Application to Web- Services for Internet Computing

He Guoand et. le proposed a Legacy systems are valuable assets for organizations. They have been evolving with new emerged technologies in rapidly changing business environment. Web Services technology and Service-Oriented Architectures (SOA) are rapidly developed and widely supported. It is a very efficient way for developers to reuse existing core business in a legacy system. Reengineering a legacy system to provide Web Services is a great challenge. A tool was developed and called Web Services Wrapper (WSW) [3]. The WSW is composed of an Analyzer and a Wrapper, which focuses on client-server legacy system with Microsoft .Net. A developer can generate Web Services and related source code according to the rules and constraints step by step with the help of WSW.The software portfolio of many organizations consists mostly of legacy systems which cannot be simply discarded for several reasons: they are the result of a huge amount of investments; they record knowledge, expertise, and business rules that may be not available anywhere else than in the source code; the costs and risks for developing a replacement system may be unaffordable and it would in any case take years before the functionality of the legacy code could be reliably replaced by the new system; the replacement of legacy code with standardized applications and ERP requires itself time and investments and not all legacy functionality can be replaced by standard packages; even when replacement systems or standard packages are available, it is indispensable to salvage the data of legacy systems.

IV) Fundamentals of deductive program synthesis

Z. Manna andet.alapproach, to construct a program meeting a given specification, the authors prove the existence of an object meeting the specified conditions. The proof is restricted to be sufficiently constructive, in the sense that, in establishing the existence of the desired output, the proof is forced to indicate a computational method for finding it. That method becomes the basis for a program that can be extracted from the proof. The exposition is based on the deductive-tableau system, a theorem-proving framework particularly suitable for program synthesis. The system includes a non-clausal resolution rule, facilities for reasoning about equality, and a well-founded induction rule. The program to meet a given specification. It focuses on the deductive approach, in which the derivation task is regarded as a problem of proving a mathematical theorem. Let us outline this approach in very general terms. We here construct only applicative (functional) programs. We are given a specification that describes a relation between the input and output of the desired program. The specification does not necessarily suggest any method for computing the output. To construct a program that meets the specification, we prove the existence, for any input object, of an output object that satisfies the specified conditions. The proof is conducted in a background theory that expresses the known properties of the subject domain and describes the primitives of the programming language. The proof is restricted to be sufficiently constructive so that, to establish the existence of a satisfactory output object, it is forced to indicate a computational method for finding one. That method becomes the basis for a program that can be extracted from the proof

All Rights Reserved © 2018 IJARMATE

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. IV, Issue IV, April 2018

V)Effective Web Service Composition in Diverse and Large-Scale Service Networks

Seog-Chan Ohand et.al proposed focus of Web services is to achieve the interoperability between distributed and heterogeneous applications. Therefore, flexible composition of Web services to fulfil the given challenging requirements is one of the most important objectives in this research field. However, until now, service composition has been largely an error-prone and difficult process. Furthermore, as the number of available web services increases, finding the right Web services to satisfy the given goal becomes intractable. In this paper, toward these issues, we propose an Artificial Intelligence[AI] planning-based framework that enables the automatic composition of Web services,and explore the following issues. First, we formulate the Web-service composition problem in terms of AI planning and network optimization problems to investigate its complexity in detail. Second, we analyses openly available Web service sets using network analysis techniques. Third, we develop a novel Web-service benchmark tool called WSBen[5]. Fourth, we develop a AI planning-based self-learn Web-service composition algorithm named WSPR. Finally, we conduct extensive experiments to verify WSPR against state-of-the-art AI planners. It is our hope that both WSPR and WSBen will provide useful information for researchers to develop Web-service discovery and composition algorithms, and software.

Related work

A)Patient Portal:

PatientPortals are health care related,online that which allow patients to communicate with theirhealthcareproviders,such as physicians and hospitals. Some patient portal applications exist as stand-alone sites and sell their services to healthcare providers. Other portal applications are integrated into the existing web site of a healthcare provider. Still other modules made into Electronic Medical Record (EMR) system. What all of these services share is the ability of patients to interact with their medical information via the Internet. Currently, the lines between an EMR, a personal health record, and a patient portal are unclear. For example, Microsoft HealthVault describe themselves as personal health records (PHRs), but they can interface with EMRs and communicate through the Record standard, displaying patient data on the Internet so it can be viewed through a patient portal

III.Techniques**:**

DataMining

Datamining is the process of identify valid,novel,potentially useful, and ultimately understandable patterns in data. With the many use of databases and the explosive growth in their sizes, organizations are faced with the problem of information overload. The problem of effectively use of these massive volumes of data is becoming a major problem or all enterprises.

Definition: Data mining or knowledge discovery in database, as it is also known, is the non-trivial extraction of implicit, previously unknown and potentially useful information from the data. This defines a number of technical approaches, such as clustering, data summarization, classification, finding dependency networks, analyzing changes, and detecting anomalies. The current evaluation of data mining functions and products is the results includes from many disciplines, including databases, information retrieval, statistics, algorithms, and machine learning

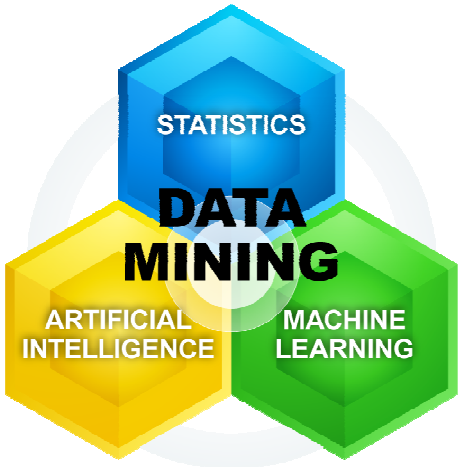


Fig. 1 Data Mining

Classification Data base,mining development are represented in the Fig. 2. The data mining system started from the year of 1960s and earlier. In this, the data mining is simply on file processing. The next stage its Database Management Systems to be started year of 1970s early to 1980s. From database management system there three broad categories to be worked. First one is Advanced Database Systems, this evaluated year of Mid-1980s to todays in this Data models and Application oriented process are worked. The Second is Data Warehousing and Data Mining worked since the year of the late 1980s to present. The third part is Web based Database Systems this started from 1990s to todays and in this Web mining and XML based database systems are included. These three broad categories are joined and create the new process that's called New generation of the Integrated Information system is started in 2000.

Data Mining Application Areas

Data mining is made in part by new applications which require new capabilities that are not currently being supplied by today's technology. These new applications can be

All Rights Reserved © 2018 IJARMATE

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. IV, Issue IV, April 2018

classified into two broad categories.

- Business and E-Commerce
- Scientific, Engineering and Health Care Data

Data Mining Tasks

Data mining tasks are mainly classified into two broad categories:

- Predictive model
- Descriptive model

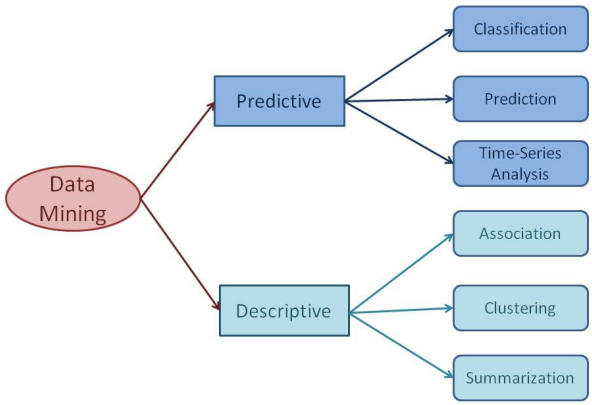


Fig2 Data Mining Clssification

I. NAÏVE BAYES CLASSIFIER

Naive Bayesis the basis have machine-learning and data mining methods. The algorithm is used to create models with predictive capabilities. It provides new ways of inspect and understanding data. It learns from the "evidence" by calculating the correlation between the target (i.e., dependent) and other (i.e., independent) variables. Neural Networks consists of three layers: input, hidden and output units (variables). The higher the weight the more important it is. Neural Network algorithms use Linear and sigmoid transfer functions. Neural Networks are suitable for training large amounts of data with few inputs. It is used when other techniques are unsatisfactory.

A. Analyzing the Data Set

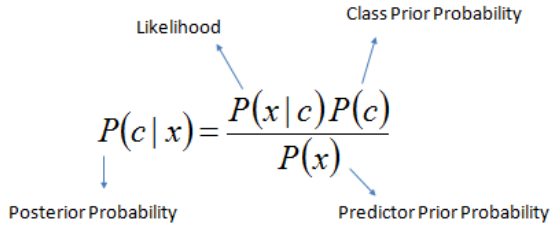
A data set (or dataset) is a collection of data, usually presented in tabular form. Each column represents a particular variable. Each row alike to a given member of the data set in question. It lists values for each of the variables, such as height and weight of an object or values of random numbers. Each value is known as a datum. The data set may fragmented to data for one or more members, to the number of rows.

The values may be numbers that are real numbers or integers, for example representing a person's height in centimeters, but may also be nominal data (i.e., not consisting of numerical values), for example representing a person's ethnicity. For each variable, the values will normally all be of the same kind. However, there may also be "missing values", which need to be indicated in some way.

A total of 500 records with 15 medical(factors) were got from the Heart Disease database lists the attributes. The records were split equally into two datasets: training dataset (455 records) and testing dataset (454 records). To avoid bias, the records for each set were selected randomly.The attribute was identified as the predictable with value "1" for patients with heart disease and value "0" for patients with no heart disease. The attribute "Patient ID" was used as the key; the rest are input attributes. It is predict that problems such as missing data, inconsistent data, and duplicate data have all been resolved. Here in project we get a data set from .dat file as source file reader program will get the data from them for the input of Naïve Bayes based mining process.

B. Naïve Bayes Theorem

Bayes theorem provides a way of calculating the posterior probability, $P(c|x)$, from $P(c)$, $P(x)$, and $P(x|c)$. Naive Bayes classifier predict that the effect of the value of a predictor (x) on a given class (c) is independent of the values of other predictors. This expectation is called class conditional independence.



$$P(c \mid \mathrm{X}) = P(x_1 \mid c) \times P(x_2 \mid c) \times \cdots \times P(x_n \mid c) \times P(c)$$

Here:

- $P(c|x)$ is the posterior probability of *class* (*target*) given *predictor* (*attribute*).
- $P(c)$ is the foregoing probability of *class*.
- $P(x|c)$ is the likelihood which is the probability of *predictor* given *class*.
- $P(x)$ is the prior probability of *predictor*.

II. AES ENCRYPTION

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES)[15]. It is found speed than triple DES.

A replacement for DES was needed as its key size was too small. With increasing calculating, it was considered weak

All Rights Reserved © 2018 IJARMATE

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. IV, Issue IV, April 2018

against all key search attack. Triple DES was designed to overcome this drawback but it was found slow.
The features of AES are as follows –

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

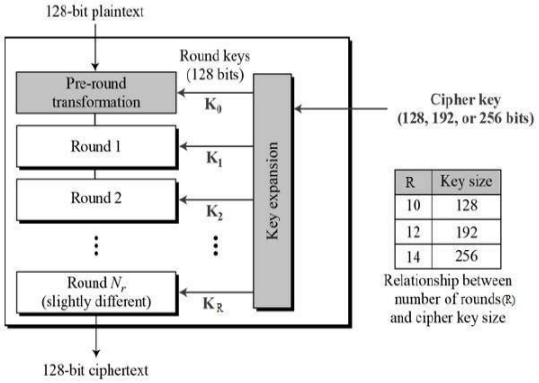
A. *Operation of AES*

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

It performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are made in four columns and four rows for processing as a matrix –

Unlike DES, the round number in AES is variable and depends on the length of the key. AES have 10 rounds for 128-bit keys and 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. It has a different 128-bit round key, which is calculated from the original AES key.

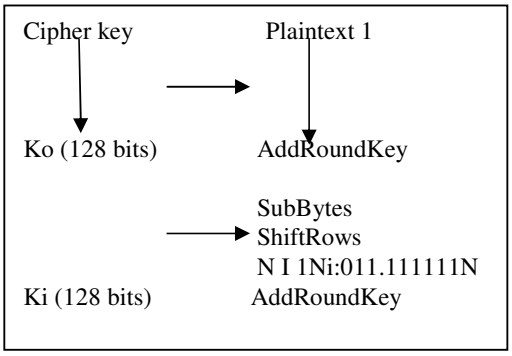
The diagramatic of AES structure is given in the following illustration



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

B–Encryption Process



Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. Thefirst round process is displayed below –

B. *Byte Substitution (Sub Bytes)*

The 16 input bytes are swapped by viewing a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

C. *Shift rows*

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows –

- First row is not shifted.
- Second row is moved one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is moved three positions to the left.

The output is a matrix has same 16 bytes but shifted with respect to each other.

D. *Mix Columns*

Each column of four bytes is now changed using a special mathematical function. This function takes as input the four bytes of one column and outputs completely new bytes, which replace the original column. The output inothernew matrix consider of 16 new bytes. It should be noted that this step is not performed in the last round.

E. *Add round key*

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

F. *Decryption Process*

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round has four processes applied in the reverse order –

- Add round key
- Mix columns
- Shift rows
- Byte substitution

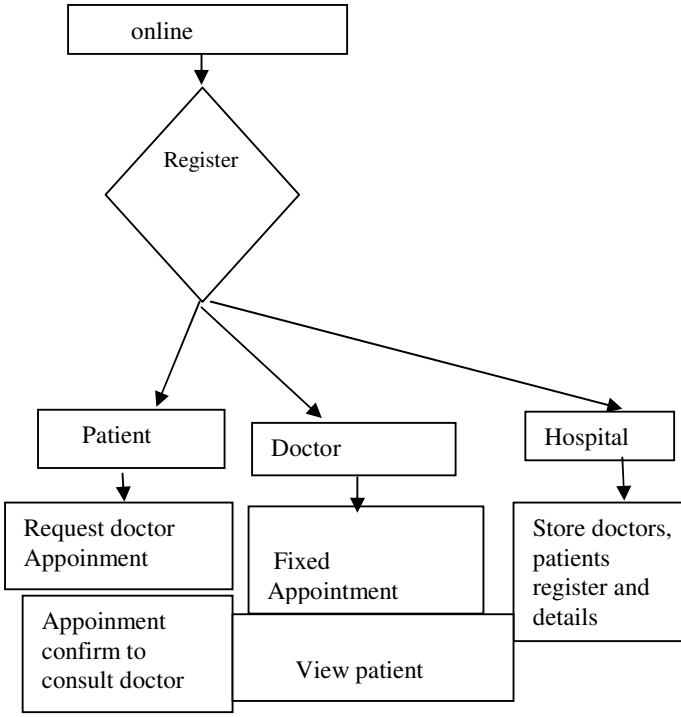
Since sub-processes in each round are in reverse manner, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.
figures. Also, do not place borders around the outside of your figures

All Rights Reserved © 2018 IJARMATE

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. IV, Issue IV, April 2018

IV)**SYSTEM ARCHITECTURE:**



REGISTRATION:

The online registration method is very easy to access the all users.Doctors, patients, are register the online system is timeless process and most of the process are done online. All details are stored in registration form.then the patients select which doctors consult the particular time.

PATIENT:

It allows public to find a doctor and schedule appointment on their convenient time and reduce waiting time in hospital. This project offers where users can view various booking slots available and select the preferred date and time. The already booked slot will be disable and will not be available for anyone else for the specified time. Cancellation, Rescheduling and finalizing appointment. SMS or Email confirmations and Reminders to patients. It allows patients to upload and download their health reports.

DOCTOR:

The doctors register the details in online health department system. View All patient registers then fixed the appointment. doctors fixed the appointment in particular date and time. Email confirmation allows doctors to upload and download their health reports.

HOSPITAL:

Registration of patient who had appointment. Capture patient's demographic details with health-related report. Cancellation, Rescheduling and finalizing appointment. Managing of patients records effortlessly. It allows upload and download patient's health reports. This module is used to have complete record of hospital employee like their address, contact number, email address, etc. It maintains the record department and category wise etc. One can search a person by name, contact number etc. In case of a doctor search by specialty.

V) CONCLUSION:

This system enables a better communication between doctor and patient, further it is used for many originations and main important of system is to identification a bogus doctor. This system can be useful for many people and identifying their solution to their health-related problem.

VI) FUTURE WORK:

This system has some features to be added into it, tracking the doctor via GPS and finding nearest location. The further we can add assessing this system through mobile by using cloud server

VII)REFERENCES

[1]. D. ARDAGNA AND B. BOND, ADAPTIVE SERVICE COMPOSITION IN FLEXIBLE PROCESSES *IEEE TRANS. SOFTWARE. ENG.*, VOL. 33, NO. 6, PP. 369–384, JUN. 2007.

[2]. Allen T. Goldberg, Knowledge-based programming: A survey of program design and construction techniques, Volume: SE-12, Issue: 7, July 1986

[3]. He Guo, Chuyan Guo, Feng Chen, Wrapping Client-Server Application to Web-Services for Internet Computing, Volume: SE-12, Issue:23 January 2006

[4].Z. Manna, R. Waldinger, Fundamentals of deductive program synthesis, Volume: SE-12, Issue:23 January 2006

[5]. Seog-Chan Oh, Dongwon Lee, Member, IEEE, and Soundar R.T. Kumara,Effective Web Service Composition in Diverse and Large-Scale Service Networks, Volume-1, NO. 1, JANUARY-MARCH 2008

[6].*N. Courtois, J. Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations", ASIACRYPT, LNCS 2501*

[7].P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", CRYPTO, LNCS 1109, pp. 104-113

[8].H. Takeuchi and N. Kodama, "Validity of association rules extracted by healthcare-data-mining,"in Proc. IEEE 36th Annu. Int. Conf. EMBC,2014,

All Rights Reserved © 2018 IJARMATE

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. IV, Issue IV, April 2018

[9]. V. Chandola, S. Sukumar, and J. Schryver, "Knowledge discovery from massive healthcare claims data,"in Proc. 19th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2013,

[10]. Meys Y. S et al (2013). Application of Smart Technologies for Mobile Patient Appointment System", International Journal of Advanced Trends in Computer Science and engineering, Vol.2(4), World Academy of Research in Science and Engineering, pp.74-85

[11]. D. Gupta, B. Denton, "Appointment scheduling in health care: challenges and opportunities", IIE Transactions, vol. 40, no. 9, pp. 800-819, 2008

[12]. Bailey, N. T. J. 1952. A study of queues and appointment systems in hospital outpatient departments, with special reference to waiting times. Journal of the Royal Statistical Society

[1 *[13]*.Cayirli, T.E. and Veral, H.R. 2006. Designing appointment sysystems for ambulatory care services. Health Care Management Science

[14].Dexter, F. 1999. Design of appointment systems to minimize patient waiting times a review of computer simulation and patient survey studies. Anesthesia and Analgesia, 89: 925–931.

[15]. Ankit K.Dandekar, Sagar Pradhan, Sagar GhormadeDesign of AES-512 Algorithm for Communication NetworkVolume: 03 Issue: 05 | May-2016

`

All Rights Reserved © 2018 IJARMATE