International Journal Of Science, Engineering, And Information Technology

Vol.1 Issue.2, July 2017

Address :
Faculty of Engineering
University of Trunojoyo Madura
Jl. Raya Telang PO BOX 2 Kamal, Bangkalan, 69192, East Java, Indonesia
Website : https://journal.trunojoyo.ac.id/ijseit

International journal of science, engineering, and information technology
Volume 01, Issue 02, July 2017
Journal homepage: https://journal.trunojoyo.ac.id/ijseit

Decision Support for Determining Children Interest and Languages Ability Using Forward-Chaining Method

Moh Haber[a], Yudha Dwi Putra Negara[b]

[a]Department of Multimedia and Network Faculty of Engineering. University of Trunojoyo Madura, Bangkalan, Indonesia
[b]Department of Informatic Engineering Faculty of Engineering. University of Trunojoyo Madura, Bangkalan, Indonesia

ABSTRACT

Early age in kindergarten is an effective age to develop various potentials and personalities possessed by children. This development effort can be done in various ways including through determination of interest. to facilitate the teachers in the process of determining a variety of different interests in each child such as constructive play, sports, exploring and entertainment, a decision support system application is needed. The decision support system analysis of determining the child's interest is carried out using the Forward Chaining method. In this application, the method is then translated into software. The software used for the grouping of areas of interest is based on data from the characteristics of each child which is then included in the rules that are made so that there will be some conclusions about each of these children. The existence of this application can help teachers in determining various kinds of interests and language progress in children.

Keywords: areas of interest, language progress, decision support, systems, forward chaining.

Article History
Received 02 February 17 Received in revised form 16 March 17 Accepted 01 April 17

1. Introduction

Early childhood, especially in kindergarten, is an effective age for developing various potentials and personalities possessed by children. This development effort can be done in various ways including through the determination of areas of interest in children.

To manage data on each of these interests, we need a method that can be used to explore the characteristics of various fields of interest. This method is known as a decision support system. With the help of software, a decision support system will conduct a data analysis process to find hidden patterns or rules within the scope of the data set of areas of interest. In this case study, this decision support system is carried out using the forward chaining method which is then translated into software.

This application was built in order to be able to provide recommendations for selected SMEs in accordance with the interests of talent in each student, the data in this application was taken from data processed from the questionnaire. After the data collection stage was completed, continued by analyzing the intelligence values of the 15 members UKM. At this stage of the analysis, we will look for the most prominent intelligence values of each UKM that are used to represent the characteristics of the UKM. At the data collection stage, the questionnaire contained 90 "Yes and No" questions for 9 intelligence categories. Every question with a value of "Yes" answered by the respondent will add one point according to the question category with a maximum of 10 points if you answer all "Yes". Searching the intelligence value of each UKM is done by calculating the Arithmetic Means value from the intelligence values obtained from the 15 respondents who represent their UKM. After the intelligence value is obtained by calculating the Arithmetic Means, the three highest multiple intelligence values are searched which will be the basis for determining the rules for [3]

2. Literature Review

2.1. Forward Chaining

Forward chaining method is a search method or forward tracking technique that starts with information that is developing rules to produce a conclusion or goal. (Russel S. Norvig P, 2003) [4]. Forward Chaining is very good if working with problems that begin with the recording of initial information and want to achieve a final solution, because the whole process will be done sequentially going forward. The following is a diagram of forward chaining in general to produce a goal.

2.2. Interest

Interest is a process that is constant to pay attention and focus on something that interests him with feelings of pleasure and satisfaction.

* *Corresponding author*
E-mail address: mohammad.khobier@gmail.com.

E-ISSN 2548-4214

Interest is a mental device consisting of a mixture of feelings, hopes, convictions, prejudices, fears or other tendencies that direct individuals to a certain thought. So, it can be concluded that interest is a development process in mixing all available abilities to direct individuals to an activity that is of interest [5].

Table 1. Interest table.

Code	Interest
M01	Playing Constructive
M02	Exploring
M03	Sport
M04	Sing / Dance

Table 2. Characteristics of habituation.

Code	Characteristics
P01	Pray before and after eating
P02	Sing a simple religious song
P03	Able to mention places of worship
P04	Able to say hello
P05	Always be friendly
P06	Carry out school rules
P07	Likes to share
P08	Helping each other friends
P09	Ability of tasks from the teacher
P10	Likes to help clean the environment
P11	Easy to get along

Table 3. Characteristics Cognitive

Code	Characteristics
K01	Being able to group objects in various ways that are known to children
K02	Able to show as many objects, plant animals that have shapes and colours
K03	Able to recognize smooth rough, light weight, short length etc.
K04	Able to pair objects according to their partners
K05	Able to numerate or mention sequence numbers
K06	Able to show 2 groups of objects that are the same, not the same, more and less
K07	Able to refer to geometric shapes
K08	Able to arrange puzzle pieces into whole shapes
K09	Able to fill containers with stones, sand etc.
K10	Able to mention additions and subtractions

Table 4. Characteristic physic and motoric.

Code	Characteristics
F01	Able to take care of himself with a little help
F02	Able to make various shapes with plasticine, playdog and clay
F03	Able to sew baste with shoelaces
F04	Able to cut freely
F05	Able to catch and throw silent balls in place
F06	Able to walk forward on the track on the catwalk board
F07	Able to jump with a height of 20-30 cm
F08	Able to climb and hang
F09	Able to take care of himself with a little help
F10	Able to make various shapes with wax, playdough and clay
F11	Able to sew baste with shoelaces

Table 5. Characteristics Art

Code	Characteristics
S01	Able to draw with media (pencils, crayons, etc.)
S02	Able to draw freely from the shapes of circles and squares
S03	Able to draw simple people completely
S04	Able to play with various musical instruments
S05	Able to colours simple drawing shapes
S06	Able to create shapes from sticks
S07	Capable of plaiting from paper
S08	Able to play colours with a variety of media
S09	Able to paint with fingers
S10	Able to sing 15 children's songs
S11	Able to recite poetry from various songs
S12	Able to make sounds from various tools

Table 6. Rule.

Rule	Code P	Code K	Code F	Code A	Interest
1	P01, P02, P08, P10, P11	K03, K04, K06, K07, K08, K09	F01, F02, F04, F08	S01, S02, S03, S05, S07, S06	M01
2	P01, P03, P04, P05, P08, P10, P11	K01, K02, K06	F01, F02, F06, F07, F08, F09, F10, F11 F12	S04, S12	M02
3	P01, P05, P04, P08, P11, P09	K09, K03, K04, K08	F05, F06, F07, F09, F10	S09, S04, S12	M03
4	P02, P04, P07, P11, P06	K05, K07, K10	F04, F10, F09	S04, S10, S11, S12	M04

3. Methods

This research methods flown like Figure 1

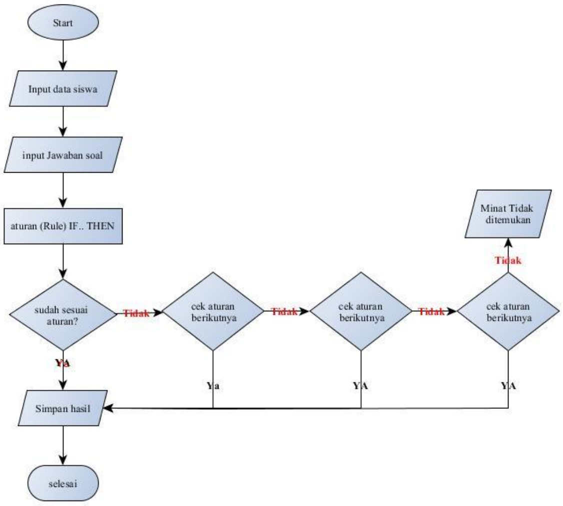
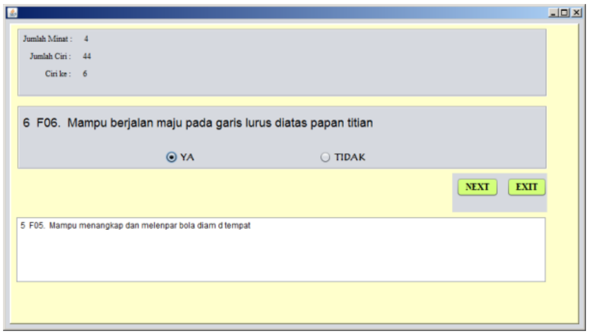


Figure 1. Research flown

4. Result

The implementation of this research was implemented in several PAUD in the ranks of the Religion Department in Bangkalan. The appearance of the application of determining interest and language progress in children is using main page, interest and determination page. On main page serves as the first interface for application / teacher program users. Main page layout shown on Figure 2. On Interest test page the teacher will answer questions about the criteria of interest, after finishing answering the question a bottom will appear to save the results, while the button exit to cancel the process and return to the main menu. Interest page shown on Figure 3. On determination interest page there are a number of buttons including: save button to overwrite new data, edit button to edit data, search button to find data, refresh button to clear columns and delete button to delete data. Figure 4 shown result page.

Figure 2. Print Screen Main page

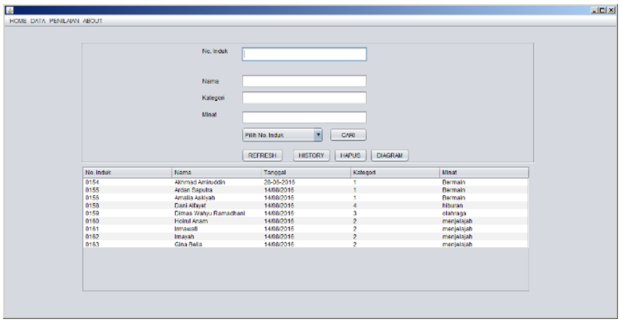

Jumlah Minat : 4
Jumlah Ciri : 44
Ciri ke : 6

6 F06. Mampu berjalan maju pada garis lurus diatas papan titian

● YA ○ TIDAK

5 F05. Mampu menangkap dan melenpar bola diam d tempat

Figure3. Print Screen Test page for determining interest



No. Induk:
Nama:
Kategori:
Minat:

No. Induk	Nama	Tanggal	Kategori	Minat
0154	Akhmad Aminuddin	28-06-2016	1	Bermain
0155	Ardan Saputra	14/08/2016	1	Bermain
0156	Amalia Askiyah	14/08/2016	1	Bermain
0158	Dani Alfayet	14/08/2016	4	hiburan
0159	Dimas Wahyu Ramadhani	14/08/2016	3	olahraga
0160	Holnil Anam	14/08/2016	2	menjelajah
0161	Immawati	14/08/2016	2	menjelajah
0162	Imayah	14/08/2016	2	menjelajah
0163	Gina Bella	14/08/2016	2	menjelajah

Figure3. Print Screen Results page of interest

5. Conclution

Based on the analysis of the system that has been produced, the following conclusions can be drawn:

- This application manages the value of the test results entered by the teacher using forward chaining.
- The output generated by this application is in the form of students and their interests determined based on the rules that have been determined.
- The rules in this application are based on case studies or the experiences of decision makers of the relevant case studies, in making decision support systems.
- In this expert system application determination of interest, the data contained in the application program can be changed or added if there is new data.

References

[1] Anharku. 2009. Simbol-simbol pada Flowchart dan Penjelasannya.

[2] Elizabeth B. Hurlock,2008, Psikologi Perkembangan, Edisi kelima, Penerbit Erlangga

[3] Levi Jordan Halim, Ranny, P.M.Winarno, 2016 Tentang “Rancang Bangun Aplikasi Penjurusan Minat Bakat Menggunakan Metode Forward Chaining”

[4] Ahmad Hoiri, Rini Agustina, 2015, “Sistem Pakar Penentuan Jenis Ekstrakurikuler Siswa Dengan Metode Forward Chaining Di Sdn Bandungrejosari 1 Sukun Lamongan”

[5] Zufrianto Wibowo, 2014, “Sistem Pendukung Keputusan Pengenal Minat Siswa Pada Bidang Ekstrakulikuler Sekolah Dengan Metode Topsis”.

[6] Hamdani, 2010, Sistem pakar untuk mendiagnosa penyakit matapada manusia.

[7] Beni wijaya, mariairmina prasetiowati, 2015, Rancang bangun system pakar untuk diagnose penyakit demam typoid dan demam berdarah dengue dengan metode forward chaining

International journal of science, engineering, and information technology
Volume 01, Issue 02, July 2017
Journal homepage: https://journal.trunojoyo.ac.id/ijseit

Implementation of View Controller Model Architecture in Population Administration Service System

Dina Mariyanti, Iwan Santosa, Eza Rahmanita

Department of Informatics Engineering, Faculty Engineering, University of Trunojoyo Madura, Bangkalan, Indonesia

ABSTRACT

Population administration services at the Kamal sub-district office are currently still using manual methods. This causes the administrative service process in the Kamal subdistrict office to not run efficiently. Therefore, an application for a web-based population administration service system is needed that is built with the Model View Controller architecture using a Codeigniter framework. Using the MVC architecture there are several benefits including software development that is easy to repair. By using the MVC architecture can bring changes that facilitate the demographic service process in the district Kamal, and can also can shorten the processing time of the service so as to reduce the buildup of queues and also facilitate the admin in the district office Kamal in the data search process of residents residing in the district Kamal. The result of the research show that MVC implementation on population administration service system applications can be easily used and developed again.

Keywords : Information System, Population Administration, Web-Based Application, MVC, Codeigniter

Article History
Received 22 February 17 Received in revised form 02 March 17 Accepted 14 April 17

1. INTRODUCTION

The Kamal sub-district office has a population administration service that helps residents to produce data. The large number of archives and residents who come often makes the population administration services run inefficiently. This is because the process of population administration services is still using the manual method. Such as making population data, archive data, civil registration data, administrative data, data generation reports and info about the sub-district of Kamal. So we need a web application that can help population administration services. The application will be built using MVC (Model View Controller) architecture.

MVC stands for Model, View, Controller, which is an architecture for creating a program. This architecture emphasizes the division of program components into three main parts, namely Model, View, and Controller [15]. The concept of MVC (Model View Controller) is a special strategy to facilitate users in the process of finding their own data, MVC is a concept that was introduced to encapsulate data along with processing (model), isolate from the process of manipulation (controller) and view (view) to be represented on a user interface [3]. So, MVC can make it easier to make large-scale applications, easy to develop, program code more neat and structured, and simplify application maintenance.

Code igniter is a framework that is very appropriate, because of its advantages, a good framework must have complete documentation, because a collection of classes without documentation is the same as a pile of foreign files and adds to the problem development, using this framework can maintain files in the application [1]. Because the files in the District Office are quite large.

Code igniter has the concept of MVC where coding is structured, namely Model as a process that interacts with the database, View as acceptance and represents data to the user, Controller functions to receive requests and data from the user and then determines what will be processed by the application [8]. Code igniter also has a library that can be used by programmers so that the program does not need to create more such as pagination libraries, session library, file uploading libraries, and others [5].

This is what drives the author to conduct a study entitled "Information System for Population Administration Services Based on Web-Based Using a View Controller Model Architecture" with a case study taken at the "Kamal District Office". Which later this application can facilitate the Kamal District Office in conducting population administration services.

2. LITERATURE REVIEW

Previous Research Previous research discusses "Design and Implementation of Web-Based Library Information Systems with MVC (Model View Controller) written by Dini Hari Pertiwi. In this study, it was concluded that the Library Information System can provide convenience for parties in the work environment in carrying out activities in the library. In the system consists of several files including; member principal files, book files, transaction files, arrangement files, stock files as well as borrowing and returning books. In the system that the author did, the time needed to produce a member data recap. book data recap,

* *Corresponding author.*
E-mail address: dina_1308@yahoo.com

membership card making, loan book recap or returned requires a relatively short time compared to the old system. And the system is made more practical because it can directly print membership cards when members confirm after registering [7]. Research conducted by Panji Wisnu Wirawan with the title "Model View Controller (MVC) Design Pattern for Java Based Device Applications". MVC design patterns can be compiled for Java / J2ME based mobile applications. Each component (Model, View and Controller) can be arranged in separate classes. With this separator, it is hoped that software components can be reusable [9]. The research entitled "Design and Analysis of Web-Based Agricultural Information Systems Using the View Controller Model Architecture" written by Michael PI Tuhuteru in 2013. In his research it can be concluded that the Agricultural Information System can help facilitate and assist the admin section in the process of inputting information data, activities , programs and production data so that they can be seen by employees or the public. Research has not been said to be perfect because it still needs some further development to get maximum results [15].

Research conducted by Wakim and Indra Sensuse Fund with the title "System Integration Model with Service Oriented Architecture (SOA) and Model View Controller (MVC) Approaches at the Indonesian Institute of Sciences Science and Technology Development Research Center" in 2017 uses REST technology that produces four services namely staffing services, asset services, inventory services and financial services. The results of this study are expected to be applied to other agencies or work units. Based on the analysis, SOA approach and MVC method function in providing integration and data exchange needs so that they can solve the problem of integrase between applications in the administration section [8].

Other research entitled "Programming View Model Framework Controller Programming Technology in Academic Advisory Information System (Case Study: STMIK Amik Riau)" by Susandri 2016. This research has successfully implemented MVC programming using an igniter framework code in the integrated academic advisory system (SIMPA) application with an existing system (e-krs and e-khs) in the Amik Riau STMIK environment [18]. b. Model View Controller Model View Controller Model is a concept that is quite popular in web application development, starting with the Small Talk programming language [4]. MVC is a model or method for creating applications by separating the data (model) from the view (view) and how to process it (controller) [2].

Model Represents the data structure of the website in the form of a database or other data, for example in the form of text files or xml files. Usually in the model will contain classes and functions to retrieve, update, and delete website data [4]. Because a website usually uses a database in storing data, the part of the model will usually relate to SQL query commands [4]. The model, is used to manage information and notify observers when information changes [3].

View is the part that regulates the display to the user. Can be said in the form of a web page [6]. As much as possible in the view does not contain the logic of the code but only contains variables that contain data ready to be displayed [4]. In the view there is no code to connect to the database. View is only devoted to displaying data from the model and controller.

Controller The controller is the link between the Model and View [14]. Inside this controller there are classes and functions that process requests from the view into the data structure in the model. The controller also does not contain code to access data [4]. His job is to accept requests sent from clients. Data requests will be processed or forwarded to other components that process data. In the end, the processed request will be submitted to the view component [2].

This MVC architecture emphasizes the division of program components into three parts namely Model, View and Controller. For a description of the MVC architecture see figure 1.

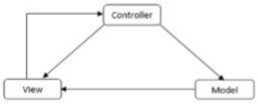


Figure 1. MVC Architecture

Information systems are tools for presenting information in such a way that it is beneficial for the recipient. The aim is to provide information in planning, initiating, organizing, operating a company that serves organizational synergy in the process of controlling decision making [11]. Population Administration

Administration includes activities that must be carried out by executive officers in an organization, whose task is to organize, advance and complete the collaborative effort of a group of people deliberately gathered to achieve certain goals.

Population is a citizen of Indonesia and foreigners who reside in Indonesia (1945 Constitution Article 26 paragraph 2). Population is a matter related to the amount, growth, distribution, mobility, distribution, quality, welfare conditions that are related to politics, economy, social, culture, religion and environment (Law No. 23 Th 2006) [13].

Population Administration is a series of structuring and controlling activities in the issuance of Population documents and data through Population Registration, Civil Registration, Population Administration information management and utilization of the results for public services and development of other sectors [10]. Definition of population administration commonly referred to as population The abbreviation Adminduk can be traced in Law Number 23 Year 2006 concerning Population Administration Article 1 which states that population administration is a series of structuring and controlling activities in the issuance of population documents and data through population registration, civil registration, management of population administration information and utilization of the results for public services and other sector development [12].

Web based application is an application that can be accessed anywhere and anytime as long as there is an internet connection [16]. Can be accessed only with a web browser, no need to install a special application to open it.

3. Methods

Population administration service information system is an application that was built to make it easier for admins in the sub-district office and make it easier for residents to see population requirements or data. In making this application adopts the MVC method with the aim of minimizing errors in the admin and can provide accurate data to the population. Division of Population Administration Services

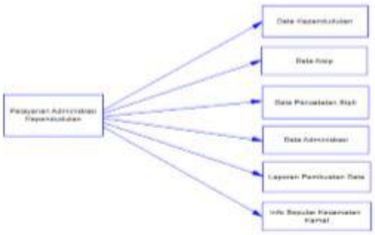


Figure 2. Population Administration Services

Population administration services include population data, archive data, civil registration data, administrative data, data generation reports and info about kamal sub-district.

4. Result

Use case diagrams are modeling to illustrate the behavior of the system to be created and can describe an interaction between one or more actors with the system. Use cases can be used to represent an interaction between user actors or other systems, so that they can simply explain the function from the user's perspective.

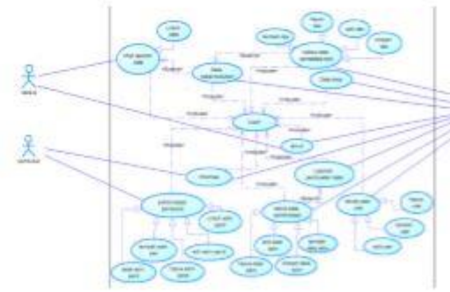


Figure 4. Usecase Diagram

MVC Implementation in Application Design shown in Figure.5

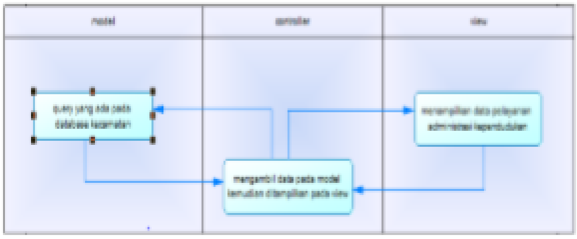

model
controller
view
query yang ada pada database kecamatan
mengambil data pada model kemudian ditampilkan pada view
menampilkan data pelayanan administrasi kependudukan

Figure 5. MVC Implementation in Application Design

Conceptual Data Model (CDM). CDM models the logical structure of the entire data application. CDM design as shown in Figure 6.

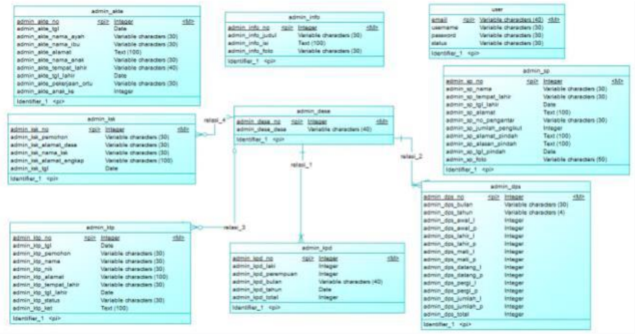


Figure 6. CDM Model

Physical Data Model (PDM) is a physical representation of the database that will be created by considering the DBMS that will be used. PDM can be generated (generated) from a CDM that was previously created. The PDM design is illustrated in Figure 7.

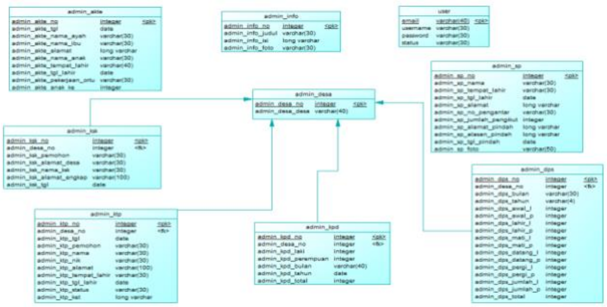


Figure 7. Physical Data Model

5. Conclusion

Based on the research that has been done, it can be concluded that:

- This study resulted in the application of Population Administration Service System using the Code Igniter framework
- This application can manage population data, administration, civil registration data, and data generation reports
- This application provides convenience for residents in the process of making population data.
- This application can be easily used and developed again.
- In the user, there is no fundamental difference if using or not using the Model View Controller architecture in the Population Administration Service System application

References

[1] Tofan Puguh Ari Kurniawan, M. I. (2012). Perancangan dan Implementasi Sistem Informasi Akademik Berbasis Web Menggunakan Arsitektur Model View Controller (MVC) (Studi Kasus: SMP Negeri 3 Bawen). 1-18.

[2] Arief Hidayat, B. S. (2012). Penerapan Arsitektur Model View Controller (Mvc) Dalam Rancang Bangun Sistem Kuis Online Adaptif. 57-64.

[3] Hidayat, A. (2012). Penerapan Arsitektur Model View Controller (MVC) Dalam Perancangan Ekstensi Sebuah Content Management System. Teknologi Informasi dan Komunikasi, 17-22.

[4] Indrianto, A. M. (2010). Penerapan Codeigniter Framework Dalam Pengembangan Sistem Informasi Sidang Keliling (Studi Kasus : Badan Peradilan Agama). 8-88.

[5] JUNAEDI, D. R. (n.d.). Penerapan Framework Codeigniter Pada Aplikasi Web E Commerce. 1-10.

[6] Pastima Simanjuntak, A. K. (Juli - Desember 2016). Analisis Model View Controller (Mvc) Pada Bahasa Php. ISD , Vol.2 No.2.

[7] Pertiwi, D. H. (2011). Desain Dan Implementasi Sistem Informasi Perpustakaan Berbasis Web Dengan Mvc (Model View Controler). teknologi dan informatika (teknomatika), 125-147.

[8] Warkim, D. I. (April 2017). Model Integrasi Sistem dengan Pendekatan Metode Service Oriented Architecture dan Model View Controller pada Pusat Penelitian Perkembangan Iptek Lembaga Ilmu Pengetahuan Indonesia. Jurnal Teknik Informatika dan Sistem Informasi, Volume 3 Nomor 1.

[9] Wirawan, P. W. (2010). ModelView-Controller (MVC) Design Pattern Untuk Aplikasi Perangkat Bergerak Berbasis Java. 1-4

[10] Setiyowati, S. S. (t.thn.). Rekayasa Ulang Proses Bisnis Pada Sistem Informasi Administrasi Kependudukan (Siak) Tingkat Kecamatan (Studi Kasus : Kecamatan Kartasura). Ilmiah SINUS , 110.

[11] WIDYASARI, Y. (2010). Analisa Perancangan Sistem Informasi Pengolahan Data Penduduk Di Kantor Camat Kecamatan Airgegas Kabupaten Bangka Selatan. 1-7.

[12] Didik Fatkhur Rohman, I. H. (2012). Implementasi Kebijakan Pelayanan Administrasi Kependudukan Terpadu (Studi pada Dinas Kependudukan dan Catatan Sipil Kota Malang). Administrasi Publik , 962-971.

[13] Faisal, A. A. (2014). Penerapan Sistem Administrasi Kependudukan (SIAK) pada Dinas Pencatatan Sipil dan Administrasi Kependudukan Kabupaten Maros. 7-50.

[14] Riduwan. 2012. Skala Pengukuran Variabel-variabel Penelitian. Bandung: Alfabeta.

[15] Michael P. I. Tuhuteru, P. I. (2013). Perancangan Dan Analisis Sistem Informasi Pertanian Berbasis Web Menggunakan Arsitektur Model View Controller. 2-25.

[16] Sagala Enjelina, E. I. (t.thn.). Rancangan Aplikasi Berbasis Web Interaktif Halloapp Berbasis Android dan iOS. 1-6.

[17] Kshirasagar Naik dan Priyadarshi Tripathy. 2011. Software Testing and Quality Assurance: Theory and Practice. John Wiley & Sons.

[18] Susandri, A. W. (2017). Teknologi Pemograman Framework Model View Controller pada Sistem Informasi Penasehat Akademis (Studi Kasus : STMIK Amik Riau). Processor , 916-925

International journal of science, engineering, and information technology
Volume 01, Issue 02, July 2017
Journal homepage: https://journal.trunojoyo.ac.id/ijseit

SMS Gateway Based Vacancy of Work Vocation Information System on Pamekasan Region

Selia Resita, Achmad Jauhari, Moch. Kautsar Sophan

Faculty of Engineering University of Trunojoyo Madura, Bangkalan, Indonesia

ABSTRACT

The increased growth of the society in Pamekasan from year to year is directly proportional to the number of job seekers increase continuesly. A large number of job seekers is not only due to the inadequate number of jobs, but also because of the slow and precise job information to the proper parties (the people who need jobs). Disnakertrans as an institution formed by the Government has made several attemps to minimize the number of job seekers, but until now the result obtained are not optimal, because there is no systemthat can accommodate the needs of both parties (providers and job seekers). Therefore, the research aims to create a website that accommodates data vacancies and job seekers. Later, the data is automatically going throught the process of weighting by means of the Simple Additive Weighting, this method is expected to optimize the selection of a job based on the latest education, gender, and age that has been mentioned by job seekers when registering. Once the selection process is complete, the job information is sent via SMS Gateway to job seekers. This SMS will send the job information suitable with the number of job seekers who have posted on the website.

Keywords: job vacancy, Simple Additive Weighting (SAW), SMS Gateway

Article History
Received 02 March 17 Received in revised form 11 March 17 Accepted 02 May 17

1. Main text

Work is an activity of doing something with the aim of getting a reward or reward in the form of money or goods. The reward is what ultimately humans use to fulfill their daily needs. Each job has its own qualifications to determine who can enter it. Pamekasan is one of the regencies in East Java with an area of 792.24 km2 and a population of 851,215 people consisting of 13 districts, 189 villages, and 178 villages [1]. Similar to other districts, Pamekasan also has various types of jobs, ranging from small industries to large companies. But not all people are able to enter the available employment. The Pamekasan Regency Manpower Office recorded that in 2011 there were 501 job seekers, in 2012 there were 690 job seekers, and in 2013 there were 3249 job seekers. This data shows quite a large number of job seekers that continue to grow from year to year.

One of the reasons for the difficulty of someone getting a job is because it is difficult to bring together job seekers with available job openings. That is because information about job vacancies is not fully received by job seekers [2]. In this case mistakes are not only made by the giver or recipient of the information, but can also be caused by the absence of an easy and affordable information distribution channel for both parties.

The social service for labor and transmigration (DISNAKERTRANS) as an institution formed by the government has a pretty heavy task in solving the unemployment problem. Some work programs that have been run by the Manpower Office to reduce the number of unemployed people are providing free training to the community, as well as collecting job seekers' data using a yellow card. However, not all government programs provide optimal results, because it is proven that every year the number of job seekers continues to grow.

To solve this problem, the authors offer a solution in the form of the use of technology that has evolved to channel information from job providers to job seekers. This technology is a website that is connected to the SMS Gateway facility. It is hoped that job vacancy information will arrive at job seekers easily, quickly, and precisely because it has gone through a selection process taken from the data of each job seeker.

2. Literature Review

My Structure Query Language(MySql) is an Open Source Relational database management system (DBMS) that is available as free software under the General Public License (GPL). The database structure is stored in related tables. Because of its open source nature, MySql can be used and distributed both for individual and corporate interests free of charge, without requiring a license from the manufacturer. Mysql can be run on a

* *Corresponding author.*
E-mail address: selia.resita1@gmail.com.

E-ISSN 2548-4214

variety of operating system platforms including Windows, Linux, Unix, Sun OS and others. MySql consists of two parts, namely Server and Client. To be able to use MySql, mysql server is first run. To run mysql server depends on the mysql operating system platform being installed. For example in Windows c: \ apache \ bin \ mysqld, while in linux / etc /rc.d/init.d/mysqld. After MySql Server is run, the mysql client program is needed to administer the mysql server, among others, creating databases, creating tables, and others [6].

PHP stands for "Hypertext Preprocessor". PHP is a scripting programming language that is placed and processed on the server. The results of the process are sent to the client, using a browser. In terms of understanding, PHP is the easiest scripting language because it has many references. PHP has 8 data types, namely boolean, integer, float / double, string, array, object, resource, and null.

The word XAMPP actually has a meaning in each letter. Like the letter X which symbolizes that this program can be run on many operating systems, such as Windows, Linux, Mac OS, and Solaris. A comes from the word Apache which functions to produce the correct web pages to users based on PHP code written by the web page creator. Apache is open source, meaning that anyone can use, take, and even change the program code. Currently the latest version of Apache is ver 2.2.41. The third and fourth letters, M and P, are derived from the words MySQL and PHP (the explanation has been explained in the previous section). The last P is an abbreviation of Perl and is a programming language that was first developed by Larry Wall. The advantage of using XAMPP is to only install once it is available and several other modules [8].

At first the Web was the information space on the internet, using hypertext technology the user was then guided to be able to find information by following the links provided in the Web document displayed by the browser. Today the internet is synonymous with the web, because it turns out that the web is able to spur the development of the internet so that with its popularity the web then becomes the standard interface for services available on the internet, from the start which was only as a provider of information until now can be used for communication such as E-mail and chatting and being able to conduct business transactions (E-Commerce), following polls, reading news and connecting to databases [9].

The SAW method is often also known as the weighted sum method. The basic concept of the SAW method is to find a weighted sum of the performance ratings for each alternative on all attributes. The SAW method requires the decision matrix normalization process (X) to a scale that can be compared with all available alternative ratings [4].

The steps in weighting with this method are as follows:

- Step 1 (Giving Criteria Weights)
- Step 2 (Weighing sub-criteria)
- Step 3 (Alternative Descriptions of each Criteria)
- Step 4 (Calculating Rating Value)

SMS Gateway is a device that offers messaging services to cellular networks from other media, or vice versa, making it possible to send or receive messages using a cell phone. An SMS Gateway system, generally consists of hardware components (servers / computers equipped with network devices) and software (applications used for message processing). And for a large system generally can use a database for data storage [10].

GNU All Mobile Management Utilities (GAMMU) is an application that can be used to manage various functions of mobile phones, modems and similar devices. GAMMU SMS Gateway is useful and very easy for us to send SMS in large quantities through a computer. Examples of applications that can be used as senders of Bulk SMS, SMS Polling, SMS Auto Reply, SMS on Demand, SMS Scheduller, and so forth.

The advantage of this API is that it allows an application with other applications to interact and interact. The programming language used by Google Maps which consists of HTML, Javascript, makes it possible to display Google Maps maps on other websites. In order for the Google Maps application to appear on certain websites, an API key is required. API key is a unique code generated by Google for a particular website, so that the Google Maps server can recognize [11].

3. Methods

Currently the Pamekasan Regency Manpower and Transmigration Office has used a website in the process of disseminating information on job vacancies as well as on jobseekers' data collection. But the website is not a special website for the people of Pamekasan Regency. This website is formed by the Department of Manpower and Transmigration (Depnakertrans) of East Java Province. The resulting output is not job search data in detail. But only limited to seeing the number of job seekers registered on the website. While complete job seeker's self data is only stored on a yellow card which certainly has a greater risk of insecurity in the storage and processing of data. The new system offered does not change the workflow too much that has been used by the Manpower Office. It is hoped that all parties concerned can use it easily. The new system flow that will be used can be seen in Figure.1

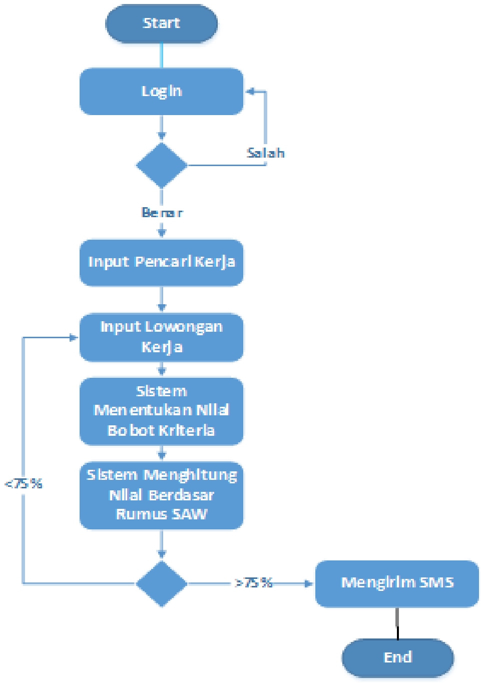
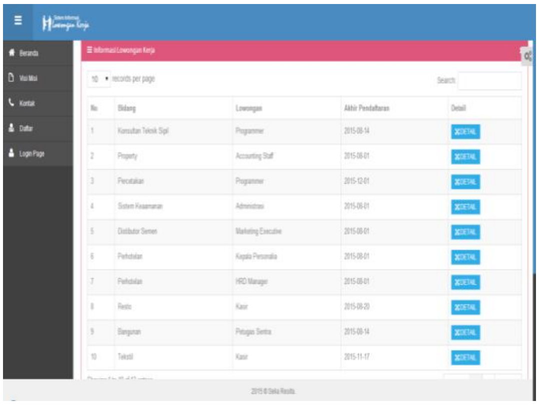


Figure 1. System flwchart

4. Implementtion

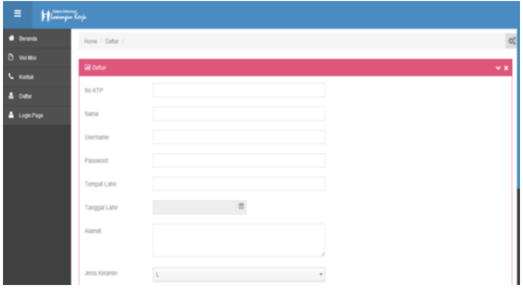
On the homepage all jobs that have been accommodated by the system will be displayed (vacancies that have been entered by the admin). On the start page, only information relating to the occupation, type of job vacancies, and the final time of registration will be displayed for those interested in registering for the vacancy. To see more detailed information, regarding the vacancies desired, system users only need to "click" details on the far right. The page views can be seen in Figure. 2



No	Bidang	Lowongan	Akhir Pendaftaran	Detail
1	Konsultan Teknik Sipil	Programmer	2015-08-14	DETAIL
2	Property	Accounting Staff	2015-08-01	DETAIL
3	Percetakan	Programmer	2015-12-01	DETAIL
4	Sistem Keamanan	Administrasi	2015-08-01	DETAIL
5	Distributor Semen	Marketing Executive	2015-08-01	DETAIL
6	Perhotelan	Kepala Personalia	2015-08-01	DETAIL
7	Perhotelan	HRD Manager	2015-08-01	DETAIL
8	Resto	Kasir	2015-08-20	DETAIL
9	Bangunan	Petugas Sentra	2015-08-14	DETAIL
10	Tekstil	Kasir	2015-11-17	DETAIL

Figure.2 Homepage

To be able to get job information easily and quickly, job seekers must first register with this system. The data fields consist of ID card number (must be Pamekasan Regency ID), name, username, password, place of birth, date of birth, address, gender, cellphone number, last education, study program, and priority (the job sought). The appearance of the job search registration form page can be seen in Figure. 3.



No KTP
Nama
Username
Password
Tempat Lahir
Tanggal Lahir
Alamat
Jenis Kelamin: L

Figure.3 Register Form

Adding work page works if the admin wants to add new job openings. Data that needs to be entered on this page consists of company name, occupation, job vacancies, recent education, majors, gender, maximum age, other information, and also the end of registration. However, please be aware that companies who want to disseminate job information through this system must be registered with the system. If the company is not yet registered, then the vacancy from that company also cannot be entered. Page views added to vacancies can be seen in Figure .4

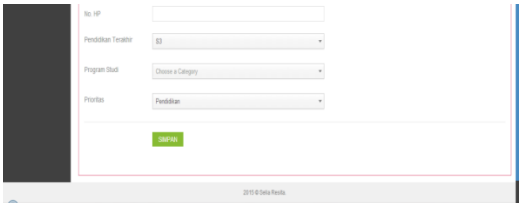

No. HP
Pendidikan Terakhir: S3
Program Studi: Choose a Category
Prioritas: Pendidikan

Figure.4 Adding work page

In the process of weighting through the SAW method it takes several steps to produce the desired value. The stages are as follows:

Step 1 (Giving Criteria Weights)

Table 1 Criteria Weights

	Criteria	Weight
C1	Education	*
C2	Gender	*
C3	Age	*

* = Weight value depends on determining job seeker's priority (50, 25, 25)

Step 2 (Weighing the sub-criteria)
L = Input job opening data
P = Input job seeker data

Table .2 Values of Educational Sub-Criteria

	Sub-Criteria	Weight
Education (P)	PL > PP	0
	PL < PP	50
	PL = PP	100

Table .3 Values of Sub-Criteria Gender

	Sub-Criteria	Weight
Gender (JK)	JKL > JKP	0
	JKL < JKP	0
	JKL = JKP	100

Table .4 Nilai Sub-Criteria Ages

	Sub-Criteria	Weight
Ages	AgeL > AgesP	100
	AgesL = AgesP	50
	AgesL < AgesP	0

Step 3 (Alternative Descriptions of each Criteria)
Alternative 1 = Contains the lowest value
Alternative 2 = Contains input values (X)
Alternative 3 = Contains the highest value

To use predetermined values, we must compare the data of job seekers and job openings. From the two data above, the following calculations can be made:

Table .5 First alternative value

Criteria	Alternative lowest	X	Highest
C1	PL > PP	PL < PP	PL = PP
C2	JKL > JKP	JKL = JKP	JKL = JKP
C3	AgesL < Ages P	AgesL > Ages P	AgesL = AgesP

Table 6 Second alternative value

	C1	C2	C3
Low	0	0	0
X	50	100	100
High	100	100	100

Step 5 (Multiled matrix (R) with weight (W))

If the higest priority on education :

V1 = (0x50) + (0x25) + (0x25) = 0

V2 = (0.5x50) + (1x25) + (1x25) = 75

V3 = (1x50) + (1x25) + (1x25) = 100

If the higest priority on gender:

V1 = (0x25) + (0x50) + (0x25) = 0

V2 = (0.5x25) + (1x50) + (1x25) = 87.5

V3 = (1x25) + (1x50) + (1x25) = 100

If the higest priority on ages:

V1 = (0x25) + (0x25) + (0x50) = 0

V2 = (0.5x25) + (1x25) + (1x50) = 87.5

V3 = (1x25) + (1x25) + (1x50) = 10

5. Conclution

The increasing number of job seekers in Pamekasan Regency is not only due to the lack of job vacancies, in this case the lack of information dissemination also still has a significant role. The absence of a system that is able to optimally reach the needs of recipients and job providers makes the writer conduct research in this field.Author builds a system as a media channeling job information that will automatically select vacancies according to personal data and the ability of job seekers. In addition, this system is also directly connected to the SMS Gateway application so that it is hoped that it will later simplify and minimize the need for time and energy for the parties concerned. System works when the first time a job seeker registers on the website, if after that there is a vacancy entered by the admin, then the selection process will begin and only job seekers who qualify for the vacancy will receive an SMS. This SMS can also play a two-way role, because job seekers can not only get SMS, but can also send SMS that will enter on the website and managed by the admin. The contents of the SMS can be in the form of notifications to stop (out) from the list of job seekers, or it can also contain criticisms and suggestions for the system used or for the Pamekasan District Manpower and Transmigration Office

REFERENCES

[1] Kemendagri. Profil Kabupaten Pamekasan. http://www.kemendagri.go.id/pages/profil-daerah/kabupaten/id/35/name/jawa-timur/detail/3528/pamekasan diakses tanggal 10 oktober 2014.

[2] Anonim. Pengertian Pengangguran dan jenis-jenisnya. http://www.ut.ac.id/html/suplemen/espa4414/isihandap.htm. diakses tanggal 10 oktober 2014.

[3] Cahyono, Dwi, dkk. Pembuatan Website Informasi Lowongan Pekerajaan. IJNS – Indonesian Journal on Networking and Security - ISSN: 2302-5700 – http://ijns.org

[4] Okaputra, Wahyu, Alif. Sistem pendukung Keputusan Kelayakan pemberian Kredit Motor Menggunakan Metode Simple Additive Weighting pada Perusahaan Leasing HD Finance. Semarang: Universitas Dian Nuswantoro. 2014.

[5] Sevani, Nina, Gisela. Aplikasi reminder pengobatan pasien berbasis sms gateway. Jakarta: INKOM, Vol. 7, No. 1, Article 215. 2013.

[6] Suryana, Tatang, Asep. Pengantar MySQL. Sumedang. 2008

[7] Khumairoh, Dururin., Munawaroh, Siti. Sistem Informasi Hrd Berbasis Web (Study Kasus : Pt.Ume Persada Indonesia,Gresik). Kerja Praktek Jurusan Teknik Informatika Fakultas Teknik Universitas Trunojoyo Madura. 2013

[8] Februariyanti, Herny, Zuliarso, Eri. Rancang Bangun Sistem Perpustakaan untuk Jurnal Elektronik. Semarang: Jurnal Teknologi Informasi DINAMIK Volume 17, No.2, Juli 2012: 124-132

[9] Setiawan, Bambang., Febriyanti, Aprilia. Impelmentasi CRM dalam Bisnis Pusat Perbelanjaan (Mall) Berbasis Web dan SMS Gateway. Surabaya: Jurnal Sistem Informasi, Volume 4, Nomor 2, hlm 100-108. 2012

[10]Rifai, Akhsin, Mustafidah, Hindayanti. Rancang Bangun Sistem Informasi Nilai Mata Pelajaran Berbasis Web dan SMS Gateway. Purwokerto: JUITA ISSN: 2086-9398 Vol. II Nomor 4, Nopember 2013.

International journal of science, engineering, and information technology
Volume 01, Issue 02, July 2017
Journal homepage: https://journal.trunojoyo.ac.id/ijseit

Data Basic Information System Based On Accreditation Based On Trunojoyo Madura University

Moch. Nasrul Ulum, M. Kautsar Sophan
Department of Informatic, Fakulty of Engineering, University of Trunojoyo Madura

ABSTRACT

The accreditation program of undergraduate study is an evaluation process which is done periodically by a body that has the authority i.e. the BANPT. The implementation of the process of preparing the accreditation program of study form of some organizations which play a role in manage and supply the data needs of the accreditation form. The data used by the program to study the process of preparation of the accreditation form is historical data collected periodically from time to time in order to give an overview of the activities/information. The process of collecting the scattered data from each of these organizations require great resources and time briefly. The system used a course at University in conducting the Madura Trunojoyo gathering historical data accreditation by searching, collecting and recording the data in its own separate list and yet maximally computerized and centralized yet most of the management and the management of its data. So it developed a system that can muster such data i.e. Information System Database-based Accrediting University Trunojoyo Madura .

Keywords: Database, Accreditation of Degree, Accreditation Forms, Information Systems, Systems Of Accreditation.

Article History
Received 12 February 17 Received in revised form 03 March 17 Accepted 02 April 17

1. Introduction

Accreditation of undergraduate study programs is an evaluation process that is carried out periodically by bodies that have the authority in the research and evaluation process namely BAN-PT so that undergraduate study programs can carry out educational programs in accordance with established standards. [1] Accreditation preparation activities, involving Educational Institutions Association which refers to the accreditation forms that have been established by BAN PT. In addition, the implementation of the process of drafting accreditation forms for study programs cannot be separated from several organizations that have a role in managing and supplying data on accreditation forms needs. The accreditation process based on these forms requires a lot of historical data and the preparation process takes a very long time. Historical data is data that is collected periodically from time to time with the aim later can provide information from an activity. [2] Historical data required for accreditation forms involves data from at least three years prior to the submission of accreditation. Historical data is very vulnerable to availability. In order to avoid losses such as data redundancy, data errors, the accuracy of the information presented, a long and long process, involving enormous resources, loss of data, and the difficulty of data management. The system used in collecting historical accreditation data from several related organizations at the University of Trunojoyo Madura by searching, collecting and recording data in their own separate lists. Based on this, a system that can manage historical data can be developed so that it becomes a data that can support the accreditation process. it is easy for the relevant agencies namely the undergraduate study program at the University of Trunojoyo Madura so that the system to be developed is expected to be able to further optimize and reduce the need for large resources in the process of collecting the accreditation historical data distribution.

2. Literature Review

Eka Kusmayadi (2008) explained in his research entitled Access and Utilization of Scientific Journal Data Base, that the database is called / called a system that can perform data collection management, whether processed manually or automatically using a computer and organized and stored in digital storage media or archive. [3] In the Academic Paper for the Accreditation of Undergraduate Study Programs (BANPT: 2008) it is explained that the Accreditation of undergraduate study programs is the process of evaluating and evaluating the quality and capacity of study programs in the organization of tertiary education programs. The assessment process to determine the feasibility of study programs in the implementation of each program is carried out by a team of colleagues who understand in detail the implementation of the study program.

An accreditation assessment element is a standard that has been set and used as a benchmark in assessing undergraduate study programs. The study program must meet each element of the assessment so that its quality can be guaranteed. The initial requirement for the assessment to be processed is to have to complete and fulfill a permit to hold a undergraduate study program from an authorized official. Accreditation assessment standards consist of seven assessment standards, namely:

* *Corresponding author.*
E-mail address: 110411100080@student.trunojoyo.ac.id

1. Vision, Mission, Objectives and Targets, and Achievement Strategies
2. Governance, Leadership, Management System and Quality Assurance
3. Students and Graduates
4. Human Resources
5. Curriculum, Learning and Academic Atmosphere
6. Financing, Facilities and Infrastructure, and Information Systems
7. Research, Services / Community Services and Collaboration

3. Design

System development model that uses the Waterfall model. The development method using Waterfall Diagram is worked out coherently for each process. If there is a process that is lacking or incompatible it will return to the previous process and so on.

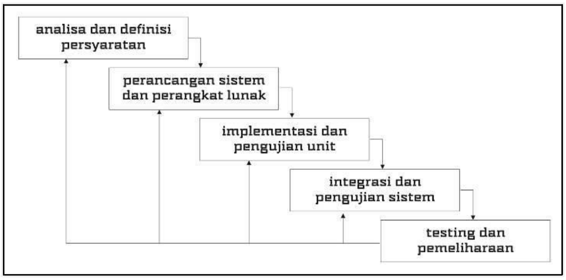

analisa dan definisi persyaratan
perancangan sistem dan perangkat lunak
implementasi dan pengujian unit
integrasi dan pengujian sistem
testing dan pemeliharaan

Figure 3.1 System Overview

System Overview

Overview of the System In the general description of the system there are three devices used in this study. The device consists of the following:
1. Client computer, whose function is to access the needs of accreditation data, besides that it is also used to
CRUD on the server side.
2. Web Server, which is used to provide web services from the server to the client.
3. Server computer, functions as a service provider for every request or request that enters the client-server. For more details about the tasks of each device can be seen in Figure 3.1 below.

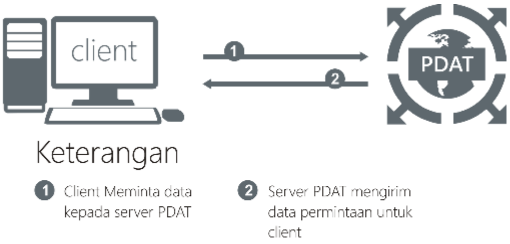
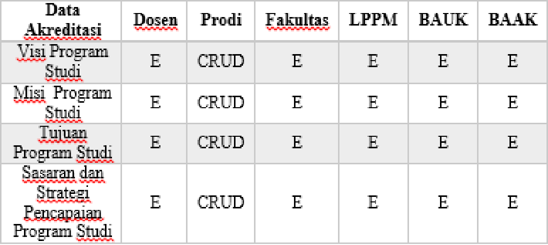

client
1
2
PDAT
Keterangan
1 Client Meminta data kepada server PDAT
2 Server PDAT mengirim data permintaan untuk client

Figure **3.2** System Overview

User matrix is used to describe and describe the type and access rights of each actor involved in the system being built. Matirks user expectations can facilitate a brief explanation of the rights or limitations of each actor in the system being built. The following is a matirks table that explains each access right in each accreditation form for undergraduate study programs



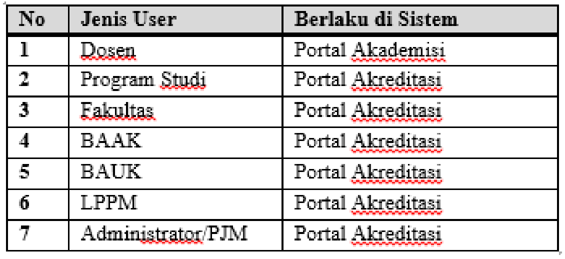
Data Akreditasi	Dosen	Prodi	Fakultas	LPPM	BAUK	BAAK
Visi Program Studi	E	CRUD	E	E	E	E
Misi Program Studi	E	CRUD	E	E	E	E
Tujuan Program Studi	E	CRUD	E	E	E	E
Sasaran dan Strategi Pencapaian Program Studi	E	CRUD	E	E	E	E

Figure 3.3 System Overview

Information:
C: Create data
R: Read data
U: Update data
D: Delet data

4. RESULTS AND DISCUSSION

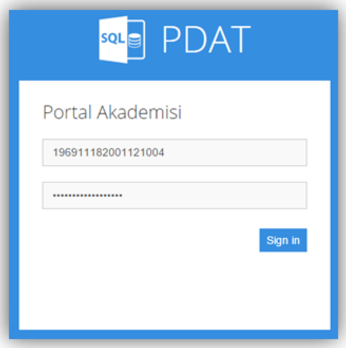
Implementation of the Database Information System for Accreditation Based Study Program of the University of Trunojoyo Madura requires a hardware that can be used as the main server to hold all data (centralized server). **I**mplementation of the system is distinguished based on two portal accesses namely the Accreditation Portal and the Academics Portal. Academic portal for Lecturer / Academic user group and accreditation portal for institutional / organizational user group.



No	Jenis User	Berlaku di Sistem
1	Dosen	Portal Akademisi
2	Program Studi	Portal Akreditasi
3	Fakultas	Portal Akreditasi
4	BAAK	Portal Akreditasi
5	BAUK	Portal Akreditasi
6	LPPM	Portal Akreditasi
7	Administrator/PJM	Portal Akreditasi

Figure 4.1 User Access Matrix Portal

Academic portal is a portal used by lecturers / academics in managing data related to Lecturers as Human Resources who also play an active role in supporting the accreditation data. The following is the login screen and home on the academics portal:



PDAT

Portal Akademisi

196911182001121004

••••••••••••••••••

Figure 4.2 Academic Portal Login Page

The accreditation portal is accessed by organizations / institutions other than related study programs as the main stakeholders in the preparation of accreditation forms which cannot be separated from the role of the preparation of accreditation forms including the Faculties, LPPM, BAUK, BAAK and the University Quality Assurance Center. The supporting data for the compilation of accreditation forms is owned by each agency / organization so that the data collection process cannot be separated from each agency / organization related to the accreditation. Each instance / organization has different access rights to the system, referring to the explanation on the access rights table previous user.

In this research, the system trial uses analysis and verification of the system design of the system that has been developed. Process features offered in system implementation towards system design design. The process refers to the user matrix which is a description of the features and access rights of each user group whether the system implementation is in accordance with the system design.

5. CONCLUSIONS

research has result in two system portals, namely a portal for Academics which includes Lecturers and a portal for organizations / institutions which include Study Programs, Faculties, LPPM, BAUK, BAAKPSI and the Trunojoyo University Madura Quality Assurance Center.

Database system built in this research can manage historical data to report presentation process to support the accreditation process.provided as part of the figure. Figures should be placed at the top or bottom of a page wherever possible, as close as possible to the first reference to them in the paper. Please ensure that all the figures are of 300 DPI resolutions as this will facilitate good output.

REFERENCES

[1] BAN-PT. Book I Academic Paper.2014

[2] Arifin, F. and Hedriyadi. Types and Data Types. September 2012. URL: http: //teorionline.net/type-and- data-type /, accessed on October 20, 2014.

[3] Kusmayadi, E. Access and Utilization of Scientific Journal Data Base. Journal of the Agricultural Library Vol. 17, Number 1. 2008.

[4] Rachmawati, A. Purpose and Benefits of the Database. May 2015. URL: https: //aullyaarvianto.wordpres s.com/2013/05/25/targeting-and- benefits-database /, accessed on December 17, 2014.

[5] BAN-PT. Book of Undergraduate Accreditation Manuscripts. Jakarta 2008.

[6] UTM. AIPT Form Trunojoyo University Madura. 2014.

[7] Nugroho, B. Making Information Systems Accreditation Forms Department D III Informatics Engineering University Eleven of March Surakarta.

[8] Foster, R. CodeIgniter 2 Cookbook. Birmingham: Packt Publishing. 2013.

[9] Orr, E. and Zadik, Y. Programming with CodeIgniter MVC. Birmingham: Packt Publishing. 2013.

[10] Upton, David. Improve your PHP coding productivity with the free compact open-source MVC CodeIgniter framework. Birmingham: Packt Publishing. 2007.

[11] Griffiths, A. CodeIgniter 1.7 Professional Development. Birmingham: Packt Publishing. 2010

International journal of science, engineering, and information technology
Volume 01, Issue 01, July 2017
Journal homepage: https://journal.trunojoyo.ac.id/ijseit

Comparative Analysis of AES-Turbo Code Combination Encryption Method on Three Variations AES Key

Rendra Bayu Adi S

Department of Informatics Engineering, Bangkalan, Indonesia

ABSTRACT

Data communication is a process of sending information from two or more points using a binary code. In data communication sometimes it does not run smoothly, while the obstacle in the process of sending information is data theft until data damage Information is exposed to noise in the process. Therefore we need an application that can provide information security and at the same time avoid damage to data due to noise. One such application is to combine AES cryptographic techniques with forward techniques error correction in the form of Turbo code. This study aims to combine the two techniques and apply to text data and analyze based on the length of the encryption key owned by AES. The analysis shows that the AES-turbo cryptographic combination algorithm can work optimally with the percentage of data returned 100% at the SNR of 15 dB. In testing the avalance effect also shows that a 256-bit key length is safer, this is evidenced by the Avalanche Effect trial of 24.77362%. But in testing the data execution time, the longer the key the longer it takes for encryption and decryption. Thus for the selection of 3 key variations of AES that are more efficient and effective, that is by using a 128-bit key.

Keywords: AES, Turbo code, AES-Turbo.

Article History
Received 12 February 16 Received in revised form 16 February 17 Accepted 03 May 17

1. Introduction

Sending or exchanging data is things that often happen in the world information technology [1]. Development rapid delivery or data exchange has an impact big, namely data security issues sent [2]. Data sent sometimes often containing important information data even very secret and must be maintained its safety. Data sending done through communication services cyberspace, usually a threat occurs so much crime. With the threat of crime such as interception, consequently data can fall on unauthorized people even data will be misused by unauthorized party [1]. other than that sometimes in data communication noise in the form of noise (3) so the data sent is vulnerable to damage. Data damage here i.e in the form of reduced or added bits the bit in the data that causes the data it was not like before sending.

To overcome some of the problems above can be done by applying a combination of cryptographic and techniques FEC (Forward Error Correction). The combination used is AES (Advanced Encryption Standard) As cryptographic techniques and Turbo Code as FEC (Forward Error Correction). AES is encryption that uses symmetric key. This standard consists of 3 block ciphers, namely AES-128, AES-192 and AES-256, which was adopted from that collection the larger one that was originally published as Rijndael. Each cipher has a 128-bit size, with a size keys are 128, 192, and 256, respectively bit [4]. Whereas Turbo Code is one of the FEC (Forward Error Correction) methods.

FEC is a method that is able to correct errors from information which is transmitted. Correction of errors is done by using coding techniques before the data is sent and before the data is received [5]. AES combination method and Turbo Code it has been studied before, namely research from Hakan CAM, Volkan OZDURAN and Osman N. UCAN named AES-Turbo. In this study explained that the two techniques can be combined by placing the turbo encoder in AES encryption in the first iteration after SubBytes and placing the decoder turbo in the AES decryption in the last iteration before SubBytes so that the process is not mutually exclusive or becomes an entity [6]. The AES-Turbo combination becomes safer because there is an encoder added to the encryption process.

This encoder also functions as an error correction as well as scrambling the bits after SubBytes. In this study, the authors used the method on the encryption side to analyze the comparison of these combinations against three key variations of AES with the test parameters namely the time required for encryption & decryption (data execution time), avalanche effects and BER (Bit Error Rate).

* *Corresponding author.*
E-mail address: 120411100038@student.trunojoyo.ac.id.

E-ISSN 2548-4214

2. Literature Review

2.1. Advanced Encryption Standard (AES)

AES is a type of cryptographic technique established by the United States standard institution called NIST (National Institute of Standards and Technology). In 2001 NIST finally published AES as a document processing standard on the FIPS-PUB 197 document. AES used a component always has an inverse with a 128-bit block length. AES key can have a key length of 128, 192,256 bits. AES encoding uses an iterative process called round. The number of rounds used by AES depends on the length of the key used. Round keys are generated based on key ones given [10]. AES supports key lengths of 128 bits to 256 bits. The key length and block size can be chosen independently, and each block is encrypted for a certain number of turns.

AES decryption algorithm is as follows first addRoundKey: X-or between states initial (ciphertext) with a cipher key. Step this is also called the initial round. Round of Nr - 1 time. That process sperformed on each round are. InvShiftRow: shift array rows wrapping state. InvSubByte: substitution of bytes with using the Inverse S- substitution table box. AddRoundKey: performs an X-or operation between the current state and the round key. InvMixColumn: randomize data on each column state array. Final round: the process for the last round:

- InvShiftRow.
- Inv SubByte.
- AddRoundKey

2.2. Turbo Code

In 1993, Berrou, and Glavieux Thitimajshima developed a canal coding techniques corrects signal errors that have been received at the receiver. Coding technique this is called Turbo Code. Turbo Code is a new paradigm for forward error-correction. This turbo code works achieve error correction performance approaching the limits of Shannon's theory. For BER value (bit error rate) 10−5 and rate code ½ required Eb / No equal to 0.7 dB [11].

The encoder consists of two encoders Recursive Systematic Convolutional (RSC) that is identical connected parallel and the second RSC encoder previously passed to a inter layer. Then the results of both The encoder is punctured, then in multiplex with information input. In the decoder, it consists of two decoders log-MAP that is connected in parallel.

Log-MAP 1 decoder input is a bit systematically received from a canal has disturbed noise $yk\ s$, redundant bit parity $yk\ p$ and feedback from the results log-MAP decoder 2 [11]. An outline of the turbo code process can be seen in Figure 1 for the encoder and 2 for decoders.

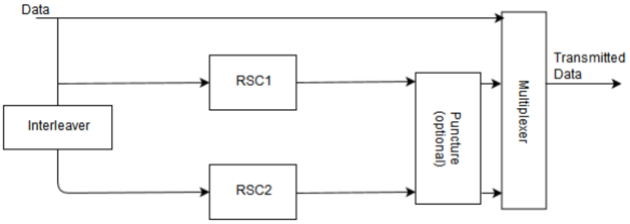


Figure 1. Turbo code encoder

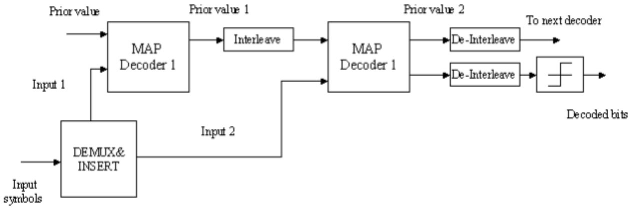


Figure 2. Turbo code decoder

3. Methods

On the encryption side there is a turbo encoder placed after sub bytes in the first iteration. In looping the first iteration of the data is entered into turbo encoder, so output data it is doubled from the data before entering the turbo encoder. Then the encoder output data it will be queued per 128 bits (in accordance with AES provisions) and at process until it becomes ciphertext, after the next 128 bits will be processed too until it becomes ciphertext and combined with the initial ciphertext. After that the bit stream is sent through wireless.

On the decryption side, the data is processed is ciphertext with a length of 256 bits (twice the length of the initial data). Then ciphertext will be processed per 128 bits and carried out the same process to Next 128 bit ciphertext. Before entering the data decoder turbo queued per 128 bits and then joined back to 256 bits and processed turbo decoder so that it becomes data 128 bit.

4. Result

Tests are carried out to see the time required for encryption & decryption (data execution time), avalanche effects and BER (Bit Error Rate).

4.1. BER performance against SNR

This trial shows the performance of BER through the ideal channel and AWGN for SNR values of 5 dB - 15 dB. This trial was conducted with 2721 characters of input data (equivalent to 1 page article), key length (128-bit, 192-bit, 256-bit), and 1 iteration.

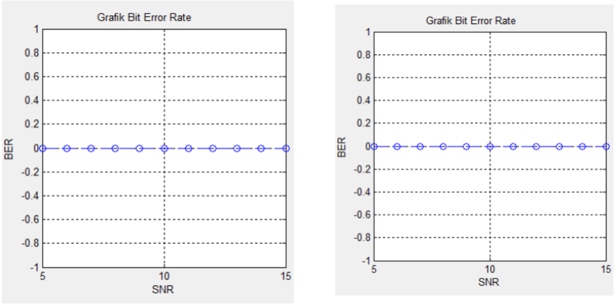


Figure 3. (a) with 128-bit key; **(b)** with 128-bit key.

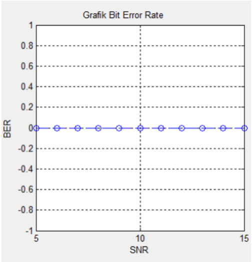


Figure 3. (c) with 256-bit key

In figure Figure 3 we can see Graph BER data text on the Ideal channel.

In Figure 4 it can be seen that the performance of BER on an ideal channel is a straight line with a Bit Error Rate value of 0 which means there is no noise in the information sent. Figure 4 BER graph in text on AWGN channel

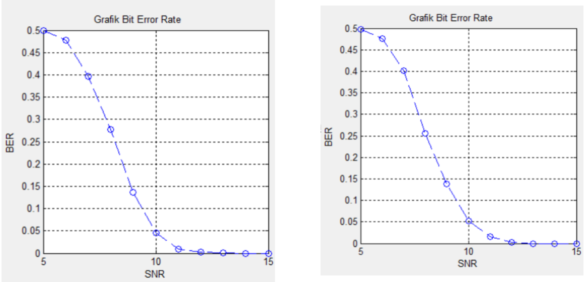


Figure 4. (a) with 128-bit key; **(b)** with 128-bit key.

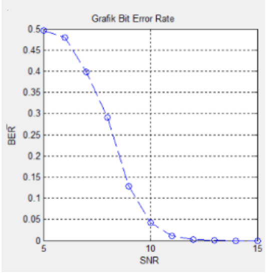


Figure 4. (c) with 256-bit key

Figure 4. shows a decrease in the bit error rate (BER) at SNR of 6 dB and stops at SNR of 13 dB, which means that at SNR more than 13 dB above data which before encryption can match the data after decryption even though it is exposed to AWGN noise.

From the data in Figure 4. the percentage of data that has been calculated is returned and is represented in Table 1.From table 1 we can see the data execution time,

- The longer the key the longer the time needed for encryption and decryption,
- The longer the data the longer the time needed for encryption and decryption,
- The time required for decryption is longer than the time required for encryption, with an average selection of 9,1878 sec.

Table 1. AES execution test table Turbo

Scenario	Key Length	Size (characters)	Time (sec)	
			Encription	Decription
		2721	40.287	42.6001
1	128	5388	71.9148	77.5686
		7826	134.252	147.08
		2721	42.3097	85.082
2	192	5388	78.5176	160.437
		7826	142.238	50.8395
		2721	46.3046	93.319
3	256	5388	83.868	93.319
		7826	156.692	177.139

5. Conclusion

From the results of research that has been done, conclusions can be drawn as follows:

- Data text (plaintext) is encrypted (ciphertext) then added noise AWGN can be decrypted back into data text (plaintext) using SNR ⩾ 15 dB.
- AES-Turbo cryptographic algorithm combination by using 3 key variations it was found that 256-bit key was safer, this is evidenced by the Avalanche trial Effect of 24.77362%. Then for encryption and decryption time in combination AES-Turbo cryptographic algorithm, increasingly key length the longer the time needed for encryption and decryption. Thus for the selection of 3 variations AES key is more efficiency and effectiveness namely by using a 128-bit key.

References

[1] Widarma, A. Kombinasi Algoritma AES, RC4 dan Elgamal dalam Skema Kriptografi Hybrid untuk Keamanan Data.Universitas Sumatera Utara.2016

[2] Kalangi, J, A. Pembuatan Aplikasi Steganography pada File Audio Mp3 dengan Metode Parity Coding.Universitas Kompter Indonesia.2010

[3] Kuswanto, Dwi. Unjuk Kerja Turbo Code pada Kanal Flat Fading. Institut Teknologi Sepuluh Nopember. 2004.

[4] National Institute of Standards and Technology. 2000. Advanced Encryption Standard, FIPS-197.

[5] Setiawan, E, F.Simulasi Kode Hamming, Kode BCH, dan Kode Reed-Solomon untuk Optimalisasi Forward Error Correction.Universitas Muhammadiyah Surakarta. 2014

[6] CAM, Hakan., OZDURAN, Volkan., Osman N. UCAN. A combined encryption and error correction scheme: AES-Turbo. Journal of electrical & electronics engineering, 1: 861-866. 2009.

[7] Darwis, Fajri. Analisis Performansi BER dengan Pengkodeaan Concatenated Viterbi / Reed-Solomon dan Turbo pada Jaringan VSAT untuk Hubungan antar BTS dan BSC. Universitas Indonesia. 2008.

[8] Marisman, Aji Fitrah, dan Hidayati, Anita. Pembangunan aplikasi pembanding kriptografi dengan Caesar chipper dan Advance Encryption Standard (AES) untuk file teks. Jurnal Penelitian Komunikasi dan Opini Publik, 19.3 . 2015.