Sample study essay

This includes collective plans and blueprints right from the conceptualization of the research project, data gathering on the existing system, knowledge requirements on different technologies included in the system, design and development of the system, up to the software evaluation.

The researcher used Prototyping as the method for development. This type of approach of evildoing the software is used for people who are usually not good at specking their requirements, nor can tell properly about what they expect from the software.

This type of System Development Method is employed when it is very difficult to obtain exact requirements from the client. While making the model, user keeps giving feedbacks from time to time and based on it, a prototype is made. The findings of this project based on all of the results gathered during the software evaluation phase were carefully tabulated and analyzed by the proponent to come up with the best possible conclusion and commendations for the betterment of the research project. The research project during the evaluation phase received an overall strongly acceptable remark from the respondents.

Keywords: Advanced Encryption Standard; Department of Education; Document Management; PKZIP; Records Management; Security, Student Grade; 1. Introduction As the immeasurable growth of technology prosper in our world, comes innovations rise up, from paper-based registration to electronic storage Of information, from the manual process of giving letters to online social media, this development cycle will remain until everybody won't seek refinement for heir lives. To increase productivity or to keep up

with everyday competition especially in the business world, you need to process everything as fast as you can.

This is where the records management system comes in, where records are in digital form and information systems are used to create, store, retrieve, distribute and dispose records.

The records management process begins with the conversion of paper documents and records to electronic files. Conversion eliminates many of the obstacles created by paper: labor- intensive duplication procedures, slow distribution, misplaced originals and he inconvenience of retrieving files from off-site storage. Because paper files are also costly to process, distribute and store, digitizing paper archives ultimately reduces operating expenses and overhead.

Records Management enables more efficient distribution of and control over information, files and records throughout an organization. These will simplify business procedures and expedite business processes by allowing instant access to information; greater collaboration within and among departments and offices; enhanced security for files and records; and the application of procedures that facilitate implicate. Furthermore, security plays an important role in the security of data.

It enables to store sensitive information or transmit it across insecure networks so that unauthorized persons cannot read it.

There is a well-known Advanced Encryption Standard (AES) or also called Rejoined is the most common encryption algorithm widely used in

applications. The Advanced Encryption Standard (AES) is well known block-cipher algorithm which is easily portable and reasonable security. For secure exchange of digital data, resulted in large quantities of different encryption algorithms this can be lassie into two groups: Symmetric encryption algorithm (with private key algorithms) and Asymmetric encryption algorithm (with public key algorithms).

Symmetric key algorithms are in general much faster to execute electronically than asymmetric key algorithms. The most commonly used symmetric encryption algorithm is AES. The input plain text and the cipher key are in state array fashion and hence known as a block cipher. The plaintext input are of fixed size, blocks of 1 28 bits and produces a block of cipher text of equal size for each plaintext block.

The most commonly used yammerer encryption algorithms are the data encryption standard (DES), triple data encryption algorithm (IDEA) and advanced encryption standard (AES).

In this research AES was implemented because it provides more secure algorithm than the others, and it is commonly used in records management system. The Department of Education in the Philippines has been collecting large volume of information for years from different schools all over the country. That information such as school and teacher profiles, student grades and promotion remarks are attached in documents or forms to be specific. There re different types of forms according to 113 educational level; Form-AAA for high schools, Form-IEEE for Grades I to Ill and Form-IEEE for Grades IV to VI.

Mainly these forms are composed of student grades and used for student promotion. Though the Department of Education has their division offices, it is still laborious to collect all of these forms. The Department of Education in the Province of Cavity covers 72 public and 310 private schools in the province they are responsible for governing and managing the basic education that includes gathering of student grades from schools under their supervision. They handle and evaluate all student grades that are inserted in all forms and process it manually.

One of the problems in this process is the lack of organization amongst the storage of forms, as time goes by, the storage area of the Division Office is now crowded with tons of folders containing information related to each school in the province of Cavity.

Another problem is that there are still forms that need to be sorted to its respective shelf. By the time they are going to search for a certain form and it is not yet properly placed, they are consuming precious time finding these forms. Also, the securities of student grade records are not secure.

Through the development of the student grade records management system for the Department of Education in the province of Cavity will modernize the process of sending required educational forms such as Form AAA, Form IEEE, Form 18-E (Report on Promotions) thru the system that will accept final grades. Routine form processes, such as reviews and approvals, can be automated paperless allowing people to collaborate easier, and reducing the time it takes to review files. Through proper workflow management, each of

these employees or canines will pass the work on according to a predetermined procedure.

Plus, the risk of losing information is reduced because electronic files are captured and managed in secured repositories. This ensures that data stored in a computer cannot be read or compromised by any individuals without authorization that mostly involves data encryption, decryption, and user access levels. The conceptual framework of the system which conveys all the required technical essentials and requirements, inputs and processes that must be accomplished for the development of the project that will then be the subject f evaluation.

This can also be considered as the visual representation that serves to explain the Structure Of the System to the users. First, the knowledge requirements play a very vital part in accomplishing the project, technical knowledge and the software development related to it.

Software and Hardware requirements were also thoroughly considered, analysis on the best possible resources were made by the researcher to ensure that the product of the project will be beneficial.

The main concern of the Process part of the diagram is to illustrate the procedures that must be undergone to ethically transform the inputs to the corresponding output that the system must generate. 114 International Journal of Sciences: Basic and Applied Research 3) volume, No 1, up 1 12-158 Fig. 1. Input process output (PIP Chart) Figure 1 depicts the conceptual framework that shows the relation of all required knowledge and technology in order to develop the e-Dog: DEPEND Student Grade Records Management

System with Implementation Of Advanced Encryption Standard and PKZIP Infrastructure.

The figure also shows how the researcher developed the research project and come up with the appropriate functions to provide services that would assist teachers, registrar, principal and the DEPEND for faster and more productive transaction. Within the development of the project, the researcher would also like the users to evaluate the system to determine what operation needs improvements. The core task of the e-Dog is to store and retrieve student grade records from individual school database to centralized database.

Securing this data from transfer to the centralized database and authenticating retrieval of data are vital to the system. Figs.

2. Security features of e-Dog Encrypted Data Transfer is one of the feature's allow the client machines to send the student grade records over to the main server for storage purposes in DEPEND Cavity. However, before the file can be transferred it must be encrypted for security purposes. This is one of the most crucial functions of the system. [26] The AES algorithm is a symmetric-key cipher, in which both the sender (Schools) and the receiver (DEPEND) uses a single key for encryption and decryption.

The length of the plain text is fixed to be 1 28 bits, while the key length can be either 128, 192, or 256 bits. The key length selected is of 128 bits. AES algorithm is an iterative algorithm. Every iteration can be called a round, and the total number of rounds is 10, 12, or 14, when key length is 1 28, 1 92, or 256 respectively. The 128 bit algorithm is divided into 16 bytes.

These bytes are represented into ex. arrays called the state array, and all the different operations of the AES algorithm such as turnarounds, subsets, shifts, miscounts and key expansion are performed on the state. 27] In AES algorithm encryption of data consists often rounds. Each round consists of four operations or transformations. Only the last round, the tenth round has only three operations to be performed. [27] 115 International Journal of Sciences: Basic and Applied Research (ISOBAR)(201 3) volume, NO 1, up 1 12-158 Figs.

3 The flow of AES. [27] A cryptographic system that uses two keys, a public key known to everyone and a private key, the private key has full control to the key owner, and has to keep in secured environment.

A unique element to the public key system is that the public and private keys are related in such a way that only the public key Can be used to encrypt messages and only the corresponding private key an be used to decrypt them. Public key cryptography was invented in 1 976 by Whitfield Edified and Martin Hellman.

It is also called asymmetric encryption because it uses two keys instead of one key (symmetric encryption). When schools send their student grade records thru e-Dog to DEPEND, The schools uses DEPEND public key to encrypt the file. DEPEND then uses her private key to decrypt it.

Using special digital signature software, the schools client machine creates a message hash (a unique numerical representation) of the transaction, uniquely identifying the data to be signed.

The school uses his riveter key to encrypt the hash. The encrypted hash becomes the digital signature of the message. The sender's certificate, digital signature and data are sent to DEPEND. If the involved parties (schools and DEPEND) aren't already using a secure connection, the sender can optionally choose to encrypt the data using the recipient's public key.

When the student grade records are received, DEPEND runs the data through the same data hashing function used by the schools.

If the data was encrypted, it is first decrypted using the recipient's private key. DEPEND uses the schools public key to decrypt the signature and the hash. If the hashes match, the integrity of the data is validated. To verify the schools' identity, the recipient checks the status of the schools' certificate.

116 volume, NO 1, up 112-158 Figs. 4. PKZIP infrastructure Problems always occur in every company on a daily basis.

But problems that are always reoccurring are the ones to be solved to maintain the reliability and integrity of the company's mission and vision.

That is why the researcher decided to aid the Department of Education in the province of Cavity that was experiencing difficulties when it comes to the annual submission of academic arms by schools. The main problems were preparation, transportation, storage and evaluation. Preparation causes confusion between teachers and school administrators whether the grades are legitimate or not.

Transportation was another main problem because faculty members of each school in the province has to find their way to the Depend Division Office just

to submit their Forms that will serve as their annual report on how well was the operation of the school in this particular school year.

Storage was another problem because copies sent by schools were kept for future purposes as ell as back up, but considering the fact that the Depend Cavity covers 72 public and 310 private schools they would need a wide space to store these documents.

Last thing was the Evaluation, by the time the Depend Cavity will conduct their evaluation they would be searching the storage room again and get these forms evaluated. This process would be time consuming and needs too much effort to execute. At the present, there is a mass of different forms like annual reports such as reports on promotions (student grade records) in the form of reports and plenty of file cabinets all over the DEPEND Cavity Division office.

As a rule, the whole reports on promotions in DEPEND are divided into three major categories: 1) reports on promotions produced and submitted by the schools in Cavity 2) reports on promotions received by DEPEND 3) legacy reports on promotions. Overall, the problems concerning the forms in the division office is summarized as follows: ; File cabinets and large file folders occupy a vast amount of the space in the division office. ; There is not any room or repository predicted for storage of the forms. Thus the distribution of the forms in the different rooms causes them to be lost, inaccessible and seed. 17 International Journal of Sciences: Basic and Applied Research (ISOBAR)(ADD 3) Volume, No 1, up 1 12-158 ; The unruly storage of the

forms, which is the consequence of lack of organizing, causes them or the content Of them to be inaccessible.

The objectives of the study alms to; improve the process of managing forms on report on promotions submitted to Department of Education in the province of Cavity; develop a model of student grade records management system that can be implemented to other DEPEND branches and schools; develop an electronic submission of student grade records (Report on

Promotion) from schools to DEPEND using the Internet; apply a robust security algorithm using Advanced Encryption Standard and PKZIP Infrastructure to secure and properly send to centralized repositories preventing unauthorized access to student grade records and; and provide fast and easy retrieval of student grade records. The study covers the DEPEND process of collecting the student grades (Report on promotions), and also recording and maintaining the final grades of all schools covered by DEPEND Cavity.

Reports covered are official forms of Form-AAA, Form-IEEE and Form-18-E. Advanced Encryption Standard is applied on this study, before the student grade records to be submitted to DEPEND; records will be encrypted and stored in the database, once retrieve to the repositories of DEPEND, student grade records will be decrypt. PKZIP Infrastructure to be included in the study.

The system considers that the system depends on human entry; human error sometimes makes information inaccurate; any disturbance or interruption during the process of inputting information would not be

recovered by the system; the system response depends on the speed of internet connection; The abundance of internet connection wouldn't be solved by the system.

The study does not cover the actual implementation of the system to DEPEND.

In this study, the beneficiary would be elementary and high school public and private schools as well as the Department of Education in the province of Cavity. This would make the operation of the Department of Education much faster due to the electronic storage and retrieving of educational forms specifically the student grades needed for promotions. This would also help the government as a whole in the concept of record management, as we all now that the government produces different kinds of records every day.

The concept of this study should be taken for consideration. As for the school staffs such as teachers and registrar, the system would benefit them in terms of passing of form AAA and EYE via online and doesn't require them to travel just to pass these forms to the Division Office in the province.

The schools and the Department of Education would also reduce their paper consumption because the storage is in electronic form. The study would improve the process of handling, storing and retrieving student grade records in DEPEND.

It will help them lessen the time and effort in passing and storing all the information of each school records in the file cabinet. DEPEND have over 13,

000 of student grade records such as Form-AAA, Form-1 EYE and Form-IEEE that must be carefully managed.

The study helps education administrators take control Of paper and electronic documents to improve efficiency, lower cost, and speed operations with Student Grades record management In addition, with instant search ability of DEPEND Form 18-A and Form 18-E, decisions can be made quicker and submission of such forms to DEPEND is easier.

Electronic access to forms in DEPEND Division Office and School Registrar reduces the need for storage and improves the speed of operational processes. Remote access to records, even from authorized people off-campus, gives educational leaders on-demand access to records without delays or costs associated with shipping. Lastly, the study will also benefit, private, public schools and DEPEND have a paperless way to manage student records.

Information is securely stored by encrypting and decrypting student grades sent by schools and shared among all components of the educational institution, from the Registrar's office, to academic departments, Development offices, DEPEND Division Office. One of the most significant steps in a research project is conducting the literature review. Through this, the readers can familiarize to the study of the researcher. The related and previous studies presented would give the readers and future researchers, an idea of the proposed system of the researcher.

The researcher selected and reviewed these studies and previous works to provide information for the readers. 118 volume 1, No 1, up 112-158

According to Gordon Information Technology (IT) is a field concerned with he use of technology in managing and processing information.

Information technology can be an important enabler of business success and innovation. This is not to say that IT equals business success and innovation or that IT represents business SUccess and innovation. Information technology is most useful when it leverages the talents of people.

Information technology in and of itself is not useful unless the right people know how to use and mange it effectively. [I] With the series development in this field of study, inventions such as Information Systems were introduced to provide solutions to enabling a systematic approach in handling information which is vital to every organization. Successfully collecting, compiling, sorting and finally analyzing information from multiple levels, in varied formats, exhibiting different granularity's can provide tremendous insight into how an organization is performing.

Taking a hard look at organizational information can yield exciting and unexpected results such as potential new markets, new ways of reaching customers, and even new ways of doing business, which is then made possible by different types Information Systems. [2] Information System is a collective set Of programs that functions to a specific purpose and are generally use to streamline the business processes and is considered by some as the backbone of every company today. It has various types such as Transaction Processing System, Office Management System, Embedded System, Management Information System and etc. 2] In this project, the

researcher developed a system that falls under the Management Information System (MIS) category.

As defined by the author, Management Information System is considered business function just as marketing, finance, operations, and human resources management are equines functions. Formally defined management information systems (MIS) is a general name for the business function and academic discipline covering the application of people, technologies and procedures-collectively called information systems- to solve business problems.

In this context, the MIS can be defined as a system that aims to consolidate the data gathered in the company and make the most out of it through a vast array of purposes and uses. [3] Part of a fully functional Information System is a great database scheme; database is a structure that contains different categories of information with their classified relationships with each other.

Determining the appropriate requirements is the key to the development of a viable database design especially in a complex type of System. 5] According to Somerville[20], security is a system attribute that reflects the ability of the system to protect itself from external attacks, which may be accidental or deliberate. These external attacks are possible because most general-purpose computers are now networked and are therefore accessible by outsiders. Examples of attacks might be the installation of viruses and Trojan horses, unauthorized use of system services or unauthorized

modification of a system or its data. In securing a system, it is best not to connect it to the Internet.

Then, the security problems are limited to ensuring that authorized users do not abuse the system. In practice, however, there are huge benefits from networked access for most large systems so disconnecting from the Internet is not cost effective. Following Somerville[20] definition and importance of security, the proponents intend to provide a security scheme for the system so as to protect the data and information stored in it. However, the security scheme will not be as sophisticated as those found in highly complex systems which requires strict confidentiality on its data.