ISSN 2278-3091
Volume 8, No.5, September - October 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse30852019.pdf
https://doi.org/10.30534/ijatcse/2019/30852019

# A Security Approach for File Management System using Data Encryption Standard (DES) algorithm

**Irma T. Plata[1], Edward B. Panganiban[1], Bryan B. Bartolome[1]**

[1]College of Computing Studies, Information and Communication Technology, Isabela State University
Echague, Isabela, Philippines, ebpanganiban@isu.edu.ph

## ABSTRACT

Security is very essential to avoid the unauthorized exposé or modification of the information. Due to the extraordinary changes in advance these days, various mixed media information is being produced and transmitted, hence, leaving our very own information defenseless against alteration and copying. Information being transmitted through a communication system can be ensured through cryptography. In an information processing environment, cryptography is executed through a process which uses a mystery key or an arrangement of bits. This paper established a security key management scheme that provides the support necessary to protect files or records between individual end users, and that also can be used to protect data stored or conveyed from one computer to another. It contains encryption and decryption process, each related with a key which should be stayed secret through Data Encryption Standard (DES). The authors employed System Development Life Cycle (SDLC), particularly on Rapid Application Development (RAD). This method involves initial data gathering, cost and requirements' analysis, and identification of the methods to be used in designing, testing, deploying and sustaining the system. Specifically, this paper used the block cipher approach as the main framework. The reliability of this system is measured using several tests done in the system. Experimental analysis includes testing in hardware and software components, system components, system units, and system integration and acceptance. The results showed that the performance of the system is in its best condition. There are four (4) parameters used in checking the complexity and time latency (CTL) in the DES algorithm. These were physical server, web server, network connectivity, and system. From each parameter, the system undergone three (3) phases of processes. Furthermore, questionnaires were floated to the respondents to assess the security system developed in terms of its usability, functionality, and reliability. The questionnaire was taken from an International Standard in evaluating system software called the ISO/IEC 25010:2011. The system was accomplished based from software tools like PHP, Apache, HTML, CSS and JavaScript for the system development and MySQL for its database. In the end, the researchers achieved high security through the implementation of DES algorithm.

**Key words:** data security, data encryption standard (DES), cryptography, file management, rapid application development

## 1. INTRODUCTION

Securing data from unkind computer users continues to be very important nowadays. Whether inhibiting unauthorized access to individual photos, data privacy compliance, or ensuring the reliability of company files, all processes require increased security to protect data from smart hackers. Particularly, a huge amount of files are stored on disk drives, the need to provide secured storage should be prioritized [1]. Storage security [2] for an application software is a must.

Nowadays, the academic individuals face a huge amount of information security occurrences such as malicious software attacks, data theft, illegal penetrations into their devices like a computer, and access to other confidential data through their links. Unfavorable impacts of these cases includes endangered significant financial losses, private data and intellectual property, and possible danger to network system, national security, and public security [3].

In any organizations, data security is a priority issue. Its application emphasizes the prevention of target availability assaults involving service refusal, and those resulting in malicious software (malware) computer viruses that enable third parties to do wrong with data and information such as exposure robbery, modification and destruction [4]. The facility in data processing and information in it should have the established security measures and the risk must be within its tolerable boundaries and must be cheap as much as possible [5].

Before, if we had to access a file or document to another computer, we would have to copy the file from an external disc and bring it to the computer on which the file was supposed to be accessed. But now we can access a file on computers placed miles away from our personal computers without copying it or bringing it in some external drive. This process of copy and paste can be removed by using the network. We can simply share the files on the cloud and these shared files at can be accessed at any place within the network without any interruption [6].

Files and folders must be kept safe in order to prevent data theft by unethical hackers. One process to secure those important files is through a cryptographic system. A cryptographic method called the Data Encryption Standard (DES) is one of the methods commonly used to secure the

delivery of services [7]. Data Encryption Standard (DES) algorithm is a method in securing data using a secret key that is very difficult to crack. There are about more than seventy two (72) quadrillion possible encryption keys can be utilized in this method. The key is chosen randomly from these combinations for each given message. Similar to existing private key cryptographic methods, both the sender and the receiver knows and use the same secret passkey.

In Isabela State University Echague Campus, the Institute of Information and Communication Technology (IICT) uses a computer based File Management System, the system enables the faculty and staff to save and retrieve a big amount of digital files and information. Though the system is proven useful it imposes a great amount of threat because of the security of digital files. The authors believed that in order to further enhance the IICT's File Management System, a certain security architecture should be applied through the use of Data Encryption Standard (DES) algorithm that will improve the security architecture of the current computer based File Management System of the Institute of Information and Communication Technology (IICT).

A File Management System is an approach which is widely used in most company, especially in the educational institutions to manage, store and safe keep their files, documents and data. Through File Management, an institution can open and retrieve the information that needs to be stored in a manner that is easy to access and reuse with the use of computers and computer related devices. Data Encryption Standard (DES) algorithm is used to secure data, where the data is encrypted into a secret key which applies a 56-bit key to each 64-bit block of data. [8].

Securing data is not a simple task to do. Data security system using DES algorithm is a Cipher Block Chaining system used to secure computer system clients and server [9]. Global reports said that millions of dollars of revenues are lost because of security issues [10]. Cryptography is about preparing cryptograms-messages or writings used to generate and recover the original information [11]. This process is difficult to implement on every device [12]. This paper presented a possible reason of why there is a need of file management in all aspects of the academe [13].

A File Based Management Information System suggests that this kind of system is needed to provide MIS solutions for small organizations that have no capability of have a huge database and with known and constant types of information needs. Some specific file structures can be designed and implemented in software applications that can be directly used by users through a simple and intuitive menu-type interface. This study suggests the need for file management in any size of institution or organization to provide decision support solutions and accurate information [14].

Electronic Record Management System focuses on bringing in organizations, a business related benefits such as enhance information sharing and increased in office productivity. Managing electronic records focuses on records reliability and authenticity. The development of ERMS is an industry response to the proliferation of electronic documents brought by digital technologies [15]. The Data Encryption Standard (DES) is the first and only openly accessible cryptographic process allowed and suggested by the United States Government [16].

These studies suggest that a computer based file management system will help improve the process of file management system using Data Encryption Algorithm security architecture (DES), a custom file management system created for the purpose of answering problems of file management of IICT.

## 2. MATERIALS AND METHODS

The System Development Life Cycle (SDLC), using Rapid Application Development (RAD) was used by authors as one of the methods in coming up with this paper. It includes preliminary investigation, requirements and cost analysis, proposed design, experimental tests, implementation and evaluation. [17].

The researchers used this methodology in developing the system because this is better and faster. Figure 1 explains this method.

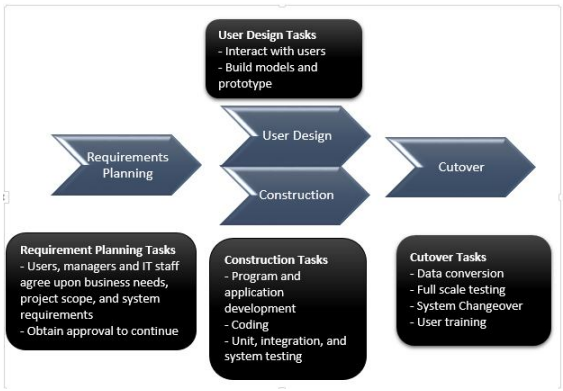


**Figure 1:** The four phases of the rapid application development model in the proposed File Management System using Data Encryption Standard algorithm

The phases of Rapid Application Development are planning the requirements, user design, system construction, and cutover tasks. The descriptive approach is also used in this paper. This permits the authors to evaluate and record all the tasks conducted. This is used to have a quantifiable information and to have a comprehensive concept of the system.

### 2.1 Conceptual Framework

Specifically, this paper used a block cipher approach as shown in figure 2. The DES block cipher encrypts a block with n-bits of data which is fixed in size. This can be 64 bits, 128 bits or 256 bits. This serves as a security gate before storing or retrieving the information. The encryption and decryption process will be performed by DES block cipher. Then the file management system will be accessed once the security process was done successfully.

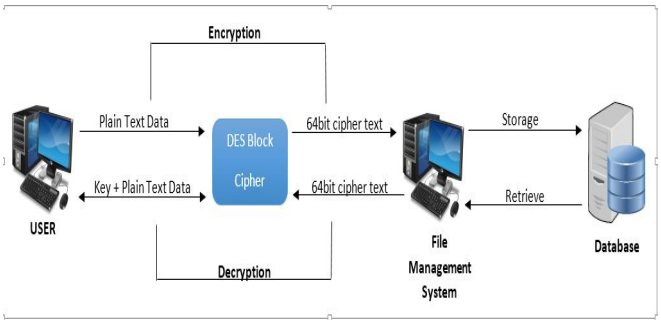


**Figure 2**: Encryption-Decryption Flow Model

### 2.2 Software Specifications

The File Management System (Using Data Encryption Standard (DES) algorithm) used MySQL, Apache, Php, HTML, Javascript and CSS as development tools. The system must be running in a Windows operating system platform. Table 1 is the list of software components that were used for the development of the system application. Details are shown indicating its specifications.

**Table 1:**. Software Specifications

| Category | Software Used |
|---|---|
| Development tools | MySQL, Apache, Php, HTML, Javascript, CSS |
| User | Windows 7 Operating System Or higher |
| Server | Windows Server 2016 Or higher |

### 2.3 Hardware Specifications

Table 2 also indicates the hardware specifications long with its recommended and minimum requirements. These are hardware materials used while developing the system.

**Table 2**: Hardware Specifications

| Category | Minimum Requirements | Recommended |
|---|---|---|
| **Server** | Windows 2016, Intel Core i5 – 7200U 2.5 GHz Intel HD Graphics Family 1760MB Memory 8GB DDR3 – Storage 500GB 15.5" HD Display, | Windows 2018 Server or higher, Intel Core i5 – 4510U 3.10GHz Intel HD Graphics Family 2.6GB AMD Radeon R5 M230 2.00GB Memory 8GB DDR4 – Storage 1TB 15.5" HD Display |
| **Client** | Windows 7 client, Intel Core i3 – 3300 3.00GHz Intel HD Graphics Family 1760MB Memory 8GB DDR3 – Storage 500GB 15.5" HD Display | Windows 8.1 or higher , Intel Core i3 – 4510U 3.10GHz Intel HD Graphics Family 2.6GB AMD Radeon R5 M230 2.00GB Memory 8GB DDR4 – Storage 1TB 15.5" HD Display |

## 3. RESULTS AND DISCUSSION

To verify the performance of the system, several tests were conducted. The results during the evaluation were tabulated in the next set of tables.

### 3.1 Hardware components testing

The results in hardware components testing were shown in table 3. This was done to attain the objectives of this paper.

**Table 3:** Testing Hardware Components

| Hardware Components | Testing #1 | Testing #2 | Remarks |
|---|---|---|---|
| **Server Computer** | The hardware needs to be set into its default setting to refresh its installed initial programs. | It is in working condition. | Restoring the hardware in its default setting gives better speed. |
| **Client Computer** | The hardware needs to be set into its default setting to refresh its installed initial programs. | It is in working condition. | Restoring the hardware in its default setting makes the system faster. |

### 3.2 Software components testing

Testing the software sets in terms of its functionalities were also established. This is shown through Table 4.

**Table 4:** Software components testing

| Software | Testing #1 | Testing #2 | Remarks |
|---|---|---|---|
| **PHP Programming Language** | Installed Successfully. | It is in working condition. | PHP 7 or its higher version is required. |
| **MySQL 5.7** | Installed Successfully. | It is in working condition. | .NET Framework 4.5 and Visual C++ Redistributable For Visual Studio |
| **MySQL Workbench Community Edition** | Installed Successfully | It is in working condition. | .NET Framework 4.5 and Visual C++ Redistributable For Visual Studio 2015 is required to function correcty |
| **Apache** | Installed Successfully | It is in working condition. | Apache httpd 2.4.34 is recommended |
| **HTML** | Installed Successfully | It is in working condition. | HTML is required to be installed in the system. |
| **CSS** | Installed Successfully | It is in working condition. | CSS2 or higher is recommended |
| **JavaScript** | Installed Successfully. | It is in working condition. | JavaScript version 1.8 or higher is recommended |

### 3.3 System components testing

The content of Table 5 is presented to verify the performance of the system components used in the project.

**Table 5:** Testing System Components

| System components | Testing #1 | Testing #2 | Remarks |
|---|---|---|---|
| **Log-in page (interface)** | The main page is working and displays the log-in page. Needs additional account. | Accounts were tested and successfully logged in. | Main page or log in page was developed and functioned correctly |
| **Account Security** | Sample intruder account was tested. The | Another intruder account was | Intruder accounts cannot enter the system. |

| | | | |
|---|---|---|---|
| | intruder account cannot penetrate the system. | tried and failed to enter the system. | Only authorized accounts can enter the system |
| **File Security** | Unauthorized account failed to open the file. | Wrong security key has failed to open the file. | Decryption key is required to open the file by authorized user |
| **All communications page** | All communications page displayed all the stored files with authorized accounts | All stored files were opened with security | The function is working properly |
| **Incoming communications page** | Incoming communications page displayed all the stored files with authorized accounts | All stored files were opened with security | The function is working properly |
| **Outgoing communications page** | Outgoing communications page displayed all the stored files with authorized accounts | All stored files were opened with security | The function is working properly |
| **Memorandum page** | Memorandum page displayed all the stored files with authorized accounts | All stored files were opened with security | The function is working properly |
| **Searching file page** | Searched files were displayed with authorized accounts | All stored files can be opened with | The function is working properly |
| **Add Accounts** | Register new accounts to use the system. | Set recovery procedure as an option for forgotten username or password | User can access the system once they are added in the user accounts |
| **Manage Database** | The system has the ability to export a database for backup reasons. | The system is capable of importing backup of the database. | This function is functioning correctly |

### 3.4 Integration and Acceptance Testing

Table 6 and 7 are the detailed representation of the integration testing and acceptance testing respectively. These tests resulted into a desirable outputs.

**Table 6 :**. Integration testing

| **Integration Testing** | | | |
|---|---|---|---|
| **Functionality** | **Testing #1** | **Testing #2** | **Remarks** |
| **Connectivity of the database to the system** | There is blocking inbound and outbound connectivity. | Exempted in the firewall. | Firewall was set into exemption to establish communication with the database. |
| **Connectivity of server to client** | Network connections successful | It is in working condition | None |

**Table 7:** Acceptance testing

| **Acceptance Testing** | | | |
|---|---|---|---|
| **Proposed Functionality** | **Trial #1** | **Trial #2** | **Remarks** |
| **Connection of the database to the server** | Connections were made possible | Connections were made possible | It is working properly. |
| **Communication of the database to the server** | Inbound and Outbound communications was successful | Communications were successful | It is working properly. |
| **Import/Export Database** | Exporting and Importing database is working correctly. | It is in proper working condition. | It is in proper working condition. |
| **Upload files in the database** | Files were successfully uploaded | It is working properly. | It is working properly. |
| **Print Files** | Files can be printed | It is working properly. | NONE |

### 3.5 System Software Evaluation

Survey questionnaires were given to the respondents to assess the usability, reliability and functionality of this paper. The questionnaire was formulated using the International Standard in evaluating software performance ISO/IEC 9126. This is now termed as ISO/IEC 25010:2011. The researchers constructed the questions but in accordance with this international standard. There are 20 respondents who answered the survey. They are the faculty and staff of IICT. These comprised of computer technician, the administrative clerk, and faculty members. These respondents were all employees from the Institute of Information and Communications Technology at Isabela State University Echague Campus.

**Table 8:** Respondents' response about the system's functionality

| **Measures** | **Weighted Average** | **Descriptive Equivalent** |
|---|---|---|
| 1. Registration of new account is successful | 4.69 | Strongly Agree |
| 2. It displays error message when registration is not successful. | 4.75 | Strongly Agree |
| 3. The system cannot accept unauthorized account. | 4.70 | Strongly Agree |
| 4. The system cannot open file with unauthorized accounts. | 4.66 | Strongly Agree |
| 5. The system has high security in protecting files | 4.78 | Strongly Agree |
| General Weighted Average | **4.73** | Strongly Agree |

Table 8 shows the tabulated response of the respondents in terms of the functionality of the system. The results showed that most of the respondents strongly agreed on the functionalities of the system with a general weighted average of 4.73.

**Table 9:** Respondents' response on the system's usability

| **Measures** | **Weighted Average** | **Descriptive Equivalent** |
|---|---|---|
| 1. The system is understandable and easy to use | 4.77 | Strongly Agree |
| 2. The system is comfortable to operate. | 4.71 | Strongly Agree |
| 3. The system has simple procedure. | 4.70 | Strongly Agree |
| 4. The system is fitted to its intended users. | 4.81 | Strongly Agree |
| 5. The system has the ability to protect files from unauthorized users | 4.82 | Strongly Agree |
| General Weighted Average | **4.76** | Strongly Agree |

When it comes to usability, the respondents evaluated the system with a general weighted mean of 4.76. This implies that the respondents strongly agreed in terms of its usability as shown in table 9.

**Table 10:** Respondents' response on the system's reliability

| Measures | Weighted Average | Descriptive Equivalent |
|---|---|---|
| 1. The system still operates when erroneous inputs occur. | 4.87 | Strongly Agree |
| 2. The system operations can be readily restored when failure occurs. | 4.78 | Strongly Agree |
| 3. The system maintains data file and folder integrity after retrieval. | 4.61 | Strongly Agree |
| 4. The system protects the data efficiently. | 4.64 | Strongly Agree |
| 5. The system has back-up and retrieval of data. | 4.80 | Strongly Agree |
| General Weighted Average | **4.74** | Strongly Agree |

Respondents also favored the system in terms of its reliability as shown in table 10. It showed a result 4.74, which indicates that the respondents strongly.

### 3.6 Performance Evaluation

The performance of this system is measured using several tests done in the system. Testing its functionalities with good output will clearly state the good performance of the system. Tests were performed in hardware and software used in the developed system. Integration, system and acceptance testing were also conducted for the detailed assessment of every units used. The results of tests were tabulated in Tables 3 to 7. The results showed that the performance of the system is in its best condition

### 3.7 Complexity and Time Latency Result

There are four (4) parameters used in checking the complexity and time latency (CTL) in the DES algorithm. These were physical server, web server, network and system. From each parameter, the system undergone three (3) phases of processes. Each parameter is explained from the figures below.

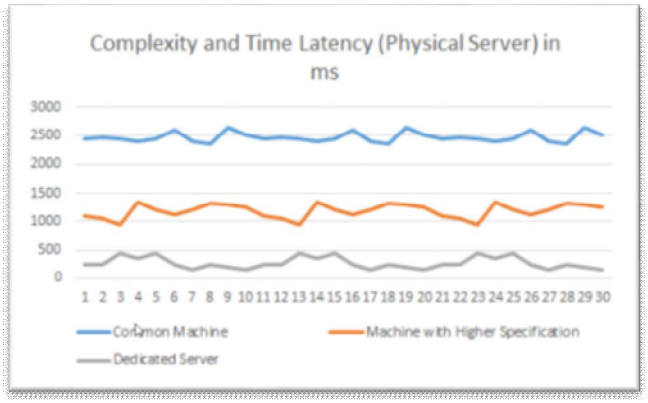


**Figure 3:** CTL (Physical Server) Test

Figure 3 demonstrates that the system undergone three phases of checking the CTL using parameter 1 (Physical Server). The authors tested how long will the system load using three different machines. At phase one, the proponents used the common machine used by the students in the laboratory with minimum hardware specification. The test resulted to an average of 2500 ms to load the system in a span of 30 seconds. The second phase, proponents used a machine with higher hardware specification and resulted to a faster output averaging 1200 ms. Lastly, the proponents used a dedicated server to test the system, and as expected, the system loads in less than a 200ms.

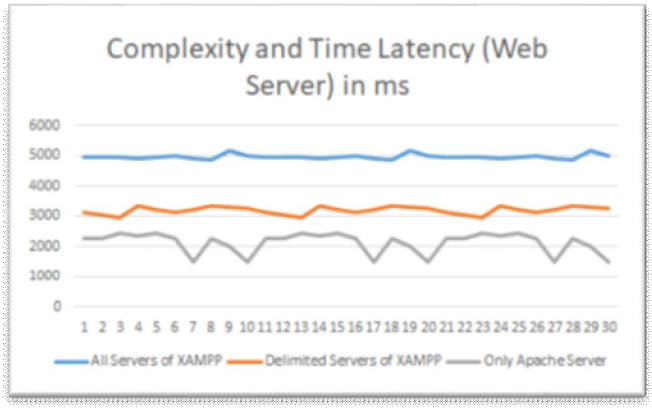


**Figure 4:** CTL (Web Server) Test

Figure 4 is about the three phases in checking the CTL using parameter 2 (Web Server). The proponents tested how long will the system load using three different machines. At phase one, the proponents run all servers included in the package of XAMPP and it resulted to more than 5000 ms to load the system. During its second phase, the proponents delimit the server running by terminating some unused server, and it resulted to a faster output with an average time of 3000 ms. For the final test, the proponents only used the apache server to run the system, and as expected, the system loads in or about 2000 ms.

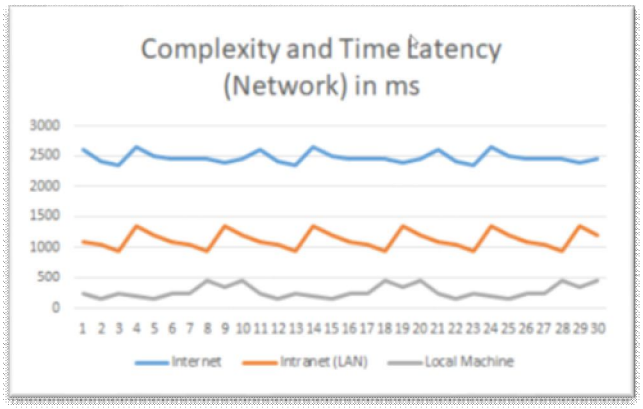


**Figure 5:**CTL (Network) Test

Figure 5 explains the three phases of checking the CTL using parameter 3 (Network). The proponents deployed the system in three modes and tested how long will the system load. At phase one, the proponents deployed over the internet and the

test resulted to 2500 ms to load the system during 30 seconds testing. The second phase, proponents only deployed in an intranet-based network and resulted to a faster output of about 1200 ms. For the last test, the proponents deployed in a local host to test the system, and as expected, the system loads in less than 500 ms.

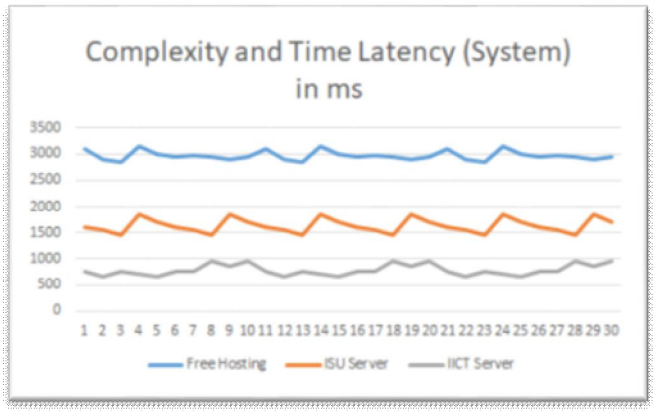


**Figure 6.** CTL (System) Test

Lastly, figure 6 is about the three phases in checking the CTL using parameter 4 (System). The proponents tested how long will the system load using three modes. At phase one, the proponents deployed the system in an open-source webhost, and it resulted to 3000 ms to load the system. The second phase, proponents deployed the system using the ISU domain and resulted to an average time of 1600 ms faster output. Finally, the proponents deployed in the IICT server, and as expected, the system loads in less than 1000 ms.

## 4. CONCLUSION

A security mechanism like cryptography increased significantly as automation improves rapidly. Data security and access control needs to be improved due to existence of computer networks with several applications like online shopping, banking, online services and many others. Thus, DES algorithm is one of the security mechanisms that the authors developed.

This paper analyzed, tested, and used crypto algorithm to come up with a File Management System. Based from several tests conducted by the authors, the integration of DES algorithm was proven to be efficient in securing data or information. Technical tests like integration, acceptance, complexity and time latency tests have proven that DES algorithm secured data from computer systems and networks. In addition, the system was graded favorably as to its usability, functionality and reliability. Through this approach, the authors achieved high security by implementing DES algorithm.

**Acknowledgment**

Special thanks to the Isabela State University Administration for the financial support that this paper has received.

## REFERENCES

[1] P. Stanton, "**Securing Data in Storage - A Review of Current Research**," 2005.

[2] B. V. Kumar, M. Ramaswami, P. Swathika, and A. Raymon, "**Wireless Body Area Network with Enhanced Object Identification , Optimal Storage and Security for Integrated Healthcare System,**" *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 3, pp. 847–853, 2019. https://doi.org/10.30534/ijatcse/2019/79832019

[3] S. A. Burd, "**The Impact of Information Security in Academic Institutions on Public Safety and Security: Assessing the Impact and Developing Solutions for Policy and Practice. Final Report,**" *Inf. Secur. Acad. Institutions Strength. Our Infrastructureand Public Saf.*, p. 254, 2006.

[4] C. Sweigart, "**Global Information Assurance Certification Paper Copyright**," 2003.

[5] R. H. Courtney, "**Security risk assessment in electronic data processing systems**," *Natl. Comput. Conf.*, pp. 97–104, 1977.

[6] S. Singh and S. Soni, "**Security of Data with 3DES & Watermarking Algorithm**," *Int. J. Futur. Revolut. Comput. Sci. Commun. Eng.*, vol. 4, no. 1, pp. 137–142, 2018.

[7] Ratnadewi, R. P. Adhie, Y. Hutama, A. Saleh Ahmar, and M. I. Setiawan, "**Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC),**" *J. Phys. Conf. Ser.*, vol. 954, no. 1, 2018. https://doi.org/10.1088/1742-6596/954/1/012009

[8] A. M. Sison, B. T. Tanguilig, B. D. Gerardo, and Y. C. Byun, "**Implementation of improved des algorithm in securing smart card data,**" *ICONS 2013 Eighth Int. Conf. Syst. Implement.*, pp. 104–110, 2013.

[9] N. Jain; G. Kaur, "**Implementing DES Algorithm in Cloud for Data Security,**" *VSRD Int. J. CS IT*, vol. 2, no. 4, pp. 316–321, 2012.

[10] C. P. Wright, M. C. Martino, and E. Zadok, "**NCryptfs: A Secure and Convenient Cryptographic File System.**," *USENIX Annu. Tech. Conf. Gen. Track*, pp. 197–210, 2003.

[11] W. F. Ehrsam, S. M. Matyas, C. H. Meyer, and W. L. Tuchman, "**A cryptographic key management scheme for implementing the Data Encryption Standard**," *Int. Bus. Mach. Corp.*, vol. 17, no. 2, pp. 106–125, 1978. https://doi.org/10.1147/sj.172.0106

[12] M. June, D. Rani, and N. S. Gill, "**Lightweight Security Protocols for Internet of Things : A Review**," *Int. J. Adv. Trends Comput. Sc ence Eng.*, vol. 8, no. 3, pp. 707–719, 2019.

https://doi.org/10.30534/ijatcse/2019/58832019

[13] S. G. T. S.R.Bharamagoudar; Geeta R.B., "**Web Based Student Information Management System**," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 2, no. 6, pp. 2342–2348, 2013.

[14] I. Moustakerov, "**A Software System for Visual Processing of Graph Data,**" *Cybern. Inf. Technol.*, vol. 5, no. 2, pp. 156–163, 2005.

[15] L. Xie, "**Computation by One-Way Multi-head Marker Automata,**" 2006.

[16] M. E. Smid and D. K. Branstad, "**Data Encryption Standard: past and future,**" *Proc. IEEE*, vol. 76, no. 5, pp. 550–559, 1988. https://doi.org/10.1109/5.4441

[17] W. B. Dittman, "**Information Systems Development,**" 2004.