DOI: 10.17148/IJARCCE.2023.12750

Digital Archival Security Design with AES Algorithm on Mail Archives

Sugiyatno[1]

Faculty of Computer Science, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia[1]

Abstract: Manual filing activities are carried out every day and sometimes it is difficult to find back documents that have been archived so that it requires a Letter archive application. The application makes it easy to collect data, archive, and search for archived letter documents. This research focuses on developing a letter archive application by implementing the AES-256 algorithm in securing letter archive files. Advanced Encryption Standard (AES) is a cryptographic algorithm that can be used to secure data. The AES algorithm is a symmetric blockchipertext that can encrypt and decrypt information. The AES algorithm uses cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. So that the AES-256 algorithm can be implemented on the current system, the help of native libraries from the go programming language is used, namely crypto/cipher and crypto/aes so that the encryption and decryption process can be applied to the letter archive file that will be archived into the application. By doing system development on the letter archive application that is currently running, it can provide a sense of trust and security to users and produce a safer archiving system than before.

Keywords: Intrution Detection System; Intrusion Prevention System; Secure Shell.

I. INTRODUCTION

Archives function as a track record of documents received by the agency or sent by the agency. Generally, archives have functions as supporting administrative activities, means of decision making, proof of accountability, sources of information, and means of communication [1].

A private university under the auspices of the Foundation has a work unit that manages documents generated every day, of course it will be very difficult to find certain documents if needed again [2]. To solve this problem, an application is needed. with the name eArchive to digitally archive documents and can facilitate searching [3]. But this letter archive application is still only limited to archiving documents and there is no further security for access to documents that have been digitally archived, and it is feared that data leakage will occur [4]..

To prevent data leakage and secure documents better, a method is needed to maintain the security of documents that have been digitally archived, namely by using cryptographic methods. In the cryptography method, there is a process called encryption, which is the disguise of data that was originally plaintext into chipertext, and there is a process called decryption, which is the opposite of encryption to convert chipertext back into plaintext. [5]

For the implementation of the encryption method in this system development will use the AES algorithm. Advanced Encryption Standard (AES) is a cryptographic algorithm that can be used to secure data. Algorithm

AES (Advanced Encryption Standard) is a symmetric blockchipertext that can encrypt and decrypt information. The AES (Advanced Encryption Standard) algorithm uses cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. The choice of data block size and key will determine the number of processes that must be passed for the encryption and decryption process. [6]

In this research, the author focuses more on document security before using and after using the AES (Advanced Encryption Standard) algorithm encryption method. Because when viewed in terms of document access rights, previously there was already a letter archive application whose access was differentiated for each work unit. Each work unit can only do read write on their respective documents [3]. For the encryption process occurs behind the application and the user will not feel the difference when accessing documents before or after applying the AES (Advanced Encryption Standard) algorithm encryption method. With the implementation of the AES (Advanced Encryption Standard) algorithm in the development of this system, it is expected that digital archiving in web-based mail archive applications will be better and safer [7].].

II. RESEARCH METHODOLOGY AND LITERATURE SURVEY

In this study, the authors used the waterfall method [8] with the following stages 1). Requirements Analysis and Definition, 2). Sytem and Software Design, 3). Implementation and Unit Testing, 4). Integration and System Testing, and 5). Operation and Maintenance.

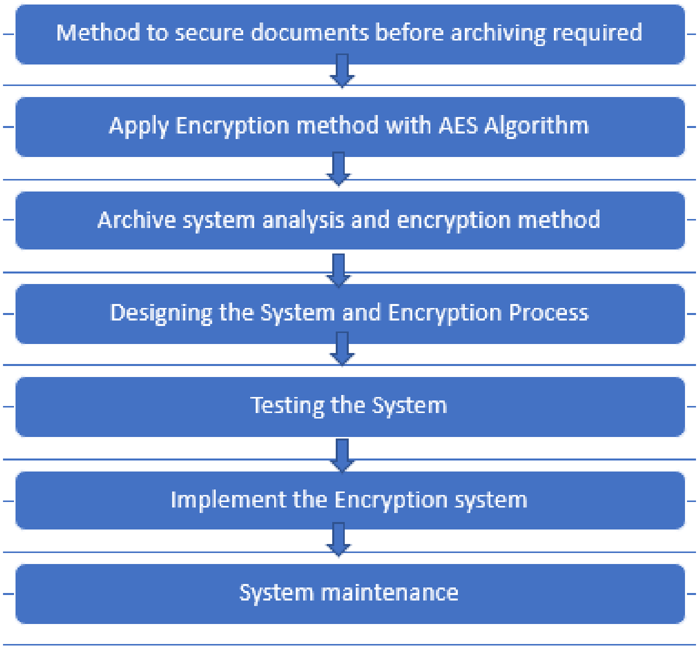
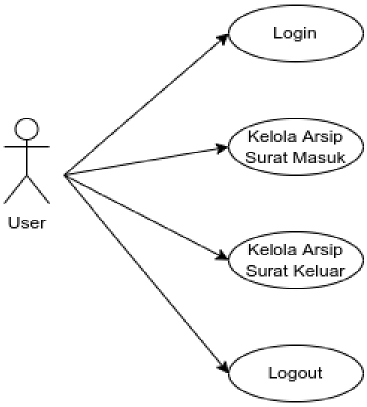

Method to secure documents before archiving required
Apply Encryption method with AES Algorithm
Archive system analysis and encryption method
Designing the System and Encryption Process
Testing the System
Implement the Encryption system
System maintenance

Figure 1. Research method (Source: Author (2022

For the system analysis stage, the author makes observations by observing and analysing how archiving works in the letter archive application. In addition to analysing the system, it is necessary to analyse the software requirements for developing applications such as programming languages using Go (Go Lang), Javascript (React.Js), Visual Studio Code, DBeaver and Google Chrome and the GNU/Linux operating system (Arch 64-bit).

After analysing the system, the researcher decides how to secure the digital archive file of the letter document when it will be uploaded or archived into the application and also when opening the digital archive file of the letter document. To overcome these problems, it is necessary to verify the user account by entering a username and password. The process of adding incoming or outgoing letter archives, by filling out the form, if there is a file in the form, the encryption process will be carried out and then the data will be stored, if there is no file, the data will be saved immediately. And for the process of opening an incoming or outgoing letter archive file, make a request to the system, followed by decrypting the file and creating a temporary URL (Uniform Resource Locator) file for files that have been decrypted in order to open files from the list of incoming or outgoing letter archives selected to be opened/displayed.



From Figure 2 above, users can perform login actions to enter the application, manage incoming mail archives (add, change, delete, view), manage outgoing mail archives (add, change, delete, view) and logout to exit the application.

Figure 2 Use Case Diagram of the System (Source: Author (2022)

DOI: 10.17148/IJARCCE.2023.12750

And here is a class diagram [9] which explains the features that exist in the system that the author will develop:

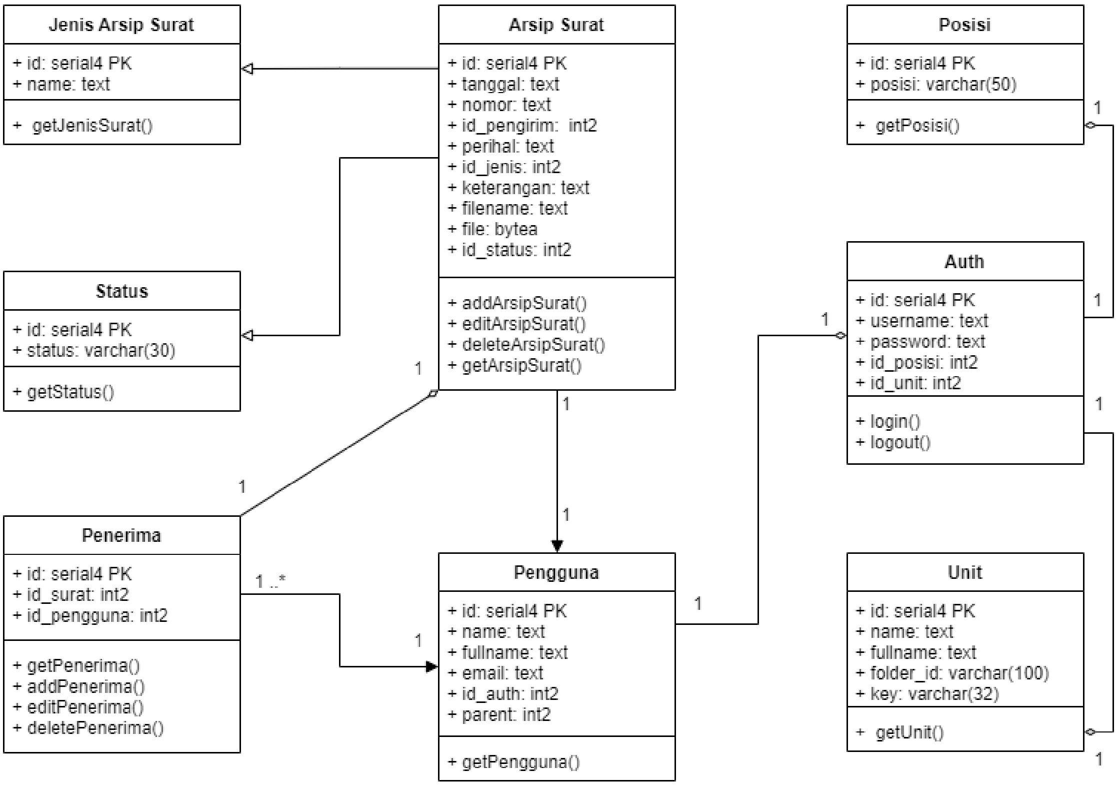


Figure 3 System Class Diagram (Source: Author (2022)

For the database design [10] that the author developed which explains the relationship between data with one another::

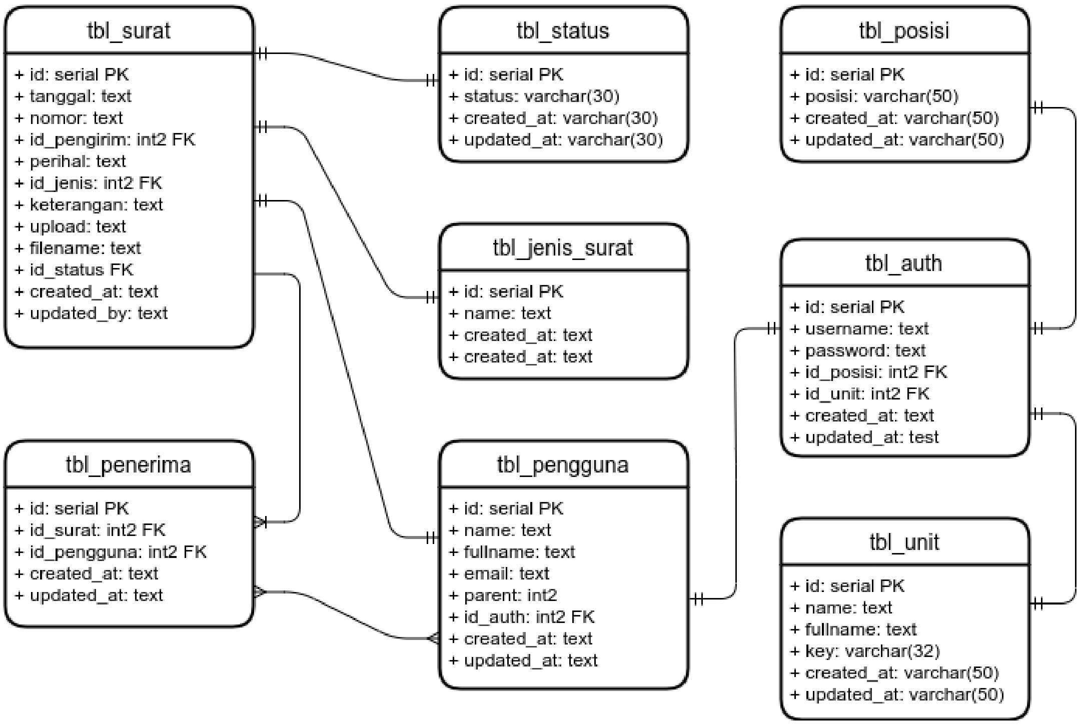


Figure 4 System Database Design (Source: Author (2022)

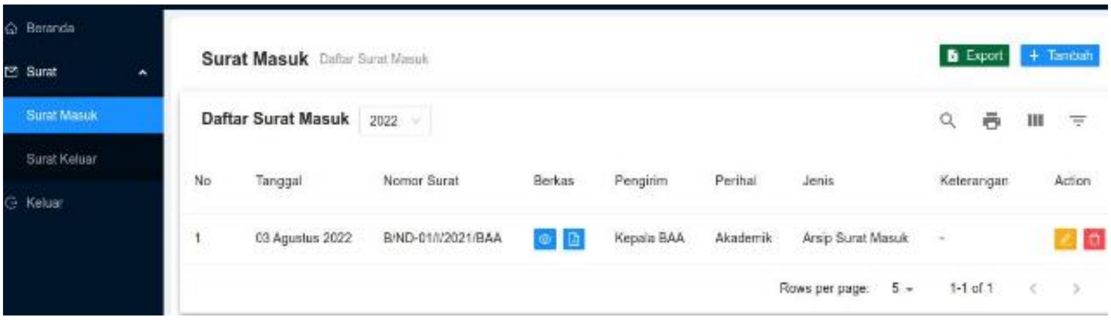
DOI: 10.17148/IJARCCE.2023.12750

III. RESULT AND DISCUSSION

To implement the AES-256 (Advanced Encryption Standard) algorithm on the developed application system, the author uses the help of the native library of the go programming language crypto/aes and crypto/cipher to perform the encryption and decryption process with the AES-256 (Advanced Encryption Standard) algorithm.

Implementation of Incoming Mail Archive Page

The incoming letter archive page is a page for managing incoming letter archive data. Users can take actions to add incoming letter archives, change incoming letter archives, delete incoming letter archives, open incoming letter archive files and export incoming letter archive data..



Surat Masuk Daftar Surat Masuk

Daftar Surat Masuk 2022

No	Tanggal	Nomor Surat	Berkas	Pengirim	Perihal	Jenis	Keterangan	Action
1	03 Agustus 2022	B/ND-01/I/2021/BAA		Kepala BAA	Akademik	Arsip Surat Masuk	-	

Rows per page: 5 1-1 of 1

Figure 5 Incoming Mail Archive Page (Source: Author (2022)

From the picture above there is text input to fill in the encryption key for the file to be archived or you can also use the generate button to generate the encryption key automatically. To see the encrypted incoming mail archive as shown below

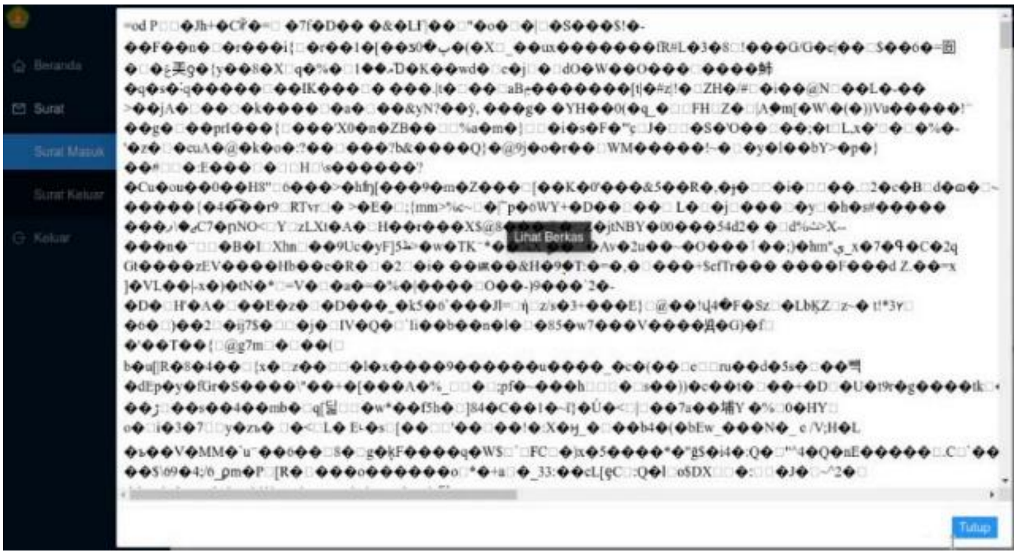


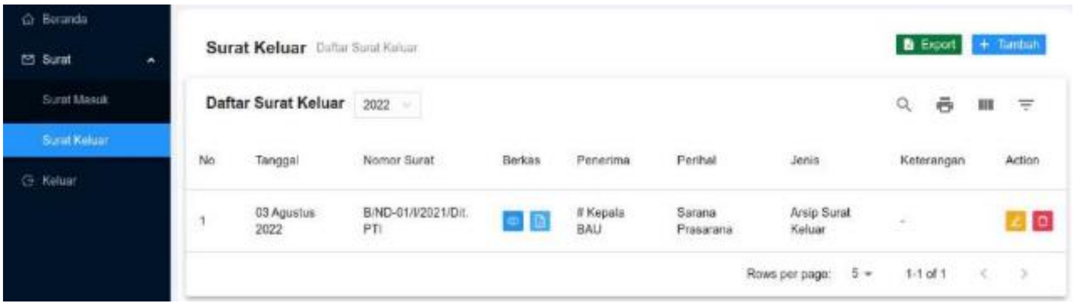
Figure 6 Result of Encryption of Incoming Mail Archive File (Source: Author (2022)

In the picture above, the encrypted outgoing letter archive file is displayed, the goal is for users to be able to confirm whether the outgoing letter archive file has been encrypted..

Implementation of the Outgoing Letter Archive Page

Similar to the incoming letter archive page, the outgoing letter archive page is used to manage outgoing letter archive data. Users can take actions to add outgoing letter archives, change outgoing letter archives, delete outgoing letter archives, open outgoing letter archive files and export outgoing letter archive data..

DOI: 10.17148/IJARCCE.2023.12750



No	Tanggal	Nomor Surat	Berkas	Penerima	Perihal	Jenis	Keterangan	Action
1	03 Agustus 2022	B/ND-01/I/2021/Dit. PTI		# Kepala BAU	Sarana Prasarana	Arsip Surat Keluar	-	

Figure 7 Outgoing Letter Archive Page (Source: Author (2022)

From Figure 7 above there is text input to fill in the encryption key for the file to be archived or you can also use the generate button to generate the encryption key automatically.

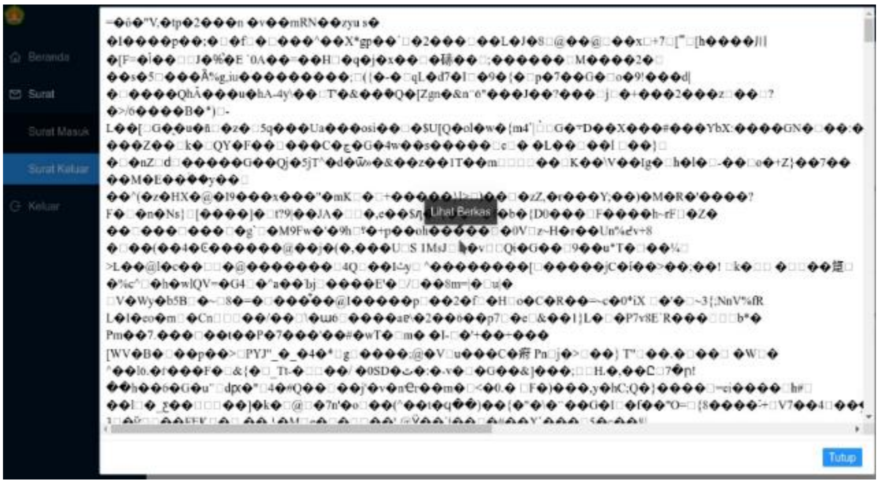
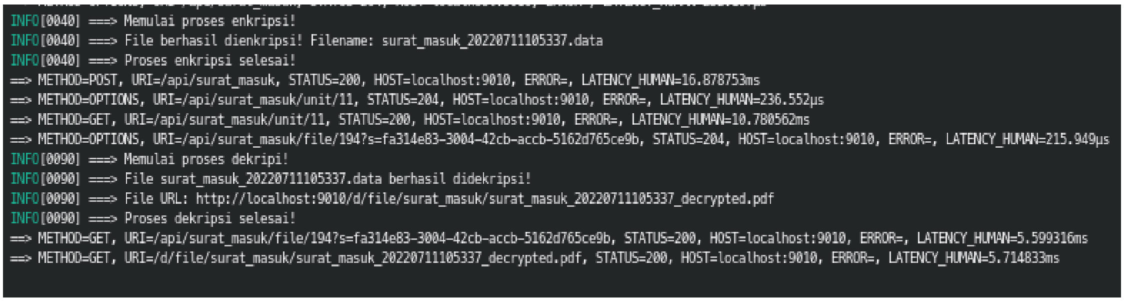


Figure 8. Outgoing Letter Archive File Encryption Results (Source: Author (2022)

AES-256 (Advanced Encryption Standard) Algorithm Testing

Testing is done to find out how the AES-256 (Advanced Encryption Standard) algorithm works and whether or not it is successful. Because all encryption and decryption processes occur in the application, the user does not feel how the encryption and decryption process runs. The following is an application log whose process occurs behind the application for the encryption and decryption process:



```
INFO[0040] ===> Memulai proses enkripsi!
INFO[0040] ===> File berhasil dienkripsi! Filename: surat_masuk_20220711105337.data
INFO[0040] ===> Proses enkripsi selesai!
==> METHOD=POST, URI=/api/surat_masuk, STATUS=200, HOST=localhost:9010, ERROR=, LATENCY_HUMAN=16.878753ms
==> METHOD=OPTIONS, URI=/api/surat_masuk/unit/11, STATUS=204, HOST=localhost:9010, ERROR=, LATENCY_HUMAN=236.552µs
==> METHOD=GET, URI=/api/surat_masuk/unit/11, STATUS=200, HOST=localhost:9010, ERROR=, LATENCY_HUMAN=10.780562ms
==> METHOD=OPTIONS, URI=/api/surat_masuk/file/194?s=fa314e83-3004-42cb-accb-5162d765ce9b, STATUS=204, HOST=localhost:9010, ERROR=, LATENCY_HUMAN=215.949µs
INFO[0090] ===> Memulai proses dekripi!
INFO[0090] ===> File surat_masuk_20220711105337.data berhasil didekripsi!
INFO[0090] ===> File URL: http://localhost:9010/d/file/surat_masuk/surat_masuk_20220711105337_decrypted.pdf
INFO[0090] ===> Proses dekripsi selesai!
==> METHOD=GET, URI=/api/surat_masuk/file/194?s=fa314e83-3004-42cb-accb-5162d765ce9b, STATUS=200, HOST=localhost:9010, ERROR=, LATENCY_HUMAN=5.599316ms
==> METHOD=GET, URI=/d/file/surat_masuk/surat_masuk_20220711105337_decrypted.pdf, STATUS=200, HOST=localhost:9010, ERROR=, LATENCY_HUMAN=5.714833ms
```

Gambar 8 Log Pengujian Aplikasi Proses Enkripsi dan Dekripsi

Comparison of File Size Before and After Encryption

The encryption process that occurs in letter archive files using the AES-256 (Advanced Encryption Standard) algorithm will certainly change the file size. Here are some examples of file size comparisons both before and after going through the encryption process

DOI: 10.17148/IJARCCE.2023.12750

Table 1 Comparison of file size before and after encryption

No	File Name	File Size (Before Encryption) (KB)	File Size (After Encryption) (KB)	File Size Increase
1	Arch Installation.pdf	43577	43605	0,99935
2	Laporan Barang AC 2 PK_.pdf	101408	101436	0,99972
3	mpdf.pdf	69364	69392	0,99959
4	Tes Upload base64 pdf.pdf	8837	8865	0,99684

IV. CONCLUSION

Based on research that can be drawn the conclusion that, the application system that has been applied to the data security method uses the AES-256 algoirtma for encryption of letter documents that will be archived using the letter archive application and decryption when accessing letter documents that have been archived into the letter archive application. With different encryption and decryption keys for each letter archive data and the key is only known by the user who created the letter archive data, the archived letter archive documents can be said to be safe. And the comparison results of the file size before and after encryption averaged 0.99%.

ACKNOWLEDGMENT

The authors thank to Universitas Bhayangkara Jakarta Raya in supporting this research as internal research grant. Also, for the reviewers who have given the insightful comments.

REFERENCES

[1] S. A. Muhidin, H. Winata, and B. Santoso, “Pengelolaan Arsip Digital.”

[2] R. Chandramouli and D. Pinhas, “Security Guidelines for Storage Infrastructure,” Gaithersburg, MD, Oct. 2020. doi: 10.6028/NIST.SP.800-209.

[3] “INTERNATIONAL COUNCIL ON ARCHIVES COMMITTEE ON BEST PRACTICES AND STANDARDS WORKING GROUP ON ACCESS Principles of Access to Archives Technical Guidance on Managing Archives with Restrictions Sample Withdrawal Sheet (Restriction Notice): Single Item Appendix D. Sample Withdrawal Sheet (Restriction Notice): Multiple Items Appendix E. Sample Withdrawal Sheet (Restriction Notice) Definitions.”

[4] A. and Libraries. Resource: The Council for Museums, Security in museums, archives and libraries : a practical guide. Resource, 2003.

[5] E. A. Vogler, Cryptography and Network Security Principles and Practices, Fourth Edition, Fourth Edi. Prentice Hall, 2016.

[6] M. W. Storer, K. Greenan, and E. L. Miller, “Long-Term Threats to Secure Archives,” 2006

[7] N. Smart, “Cryptography: An Introduction (3rd Edition).”

[8] D. Dalcher, Going Beyond The Waterfall: Managing Scope Effectively Across the Project Life Cycle, vol. 46, no. 1. 2015. doi: 10.1002/pmj.21475.

[9] S. Kölbl, “Design and analysis of cryptographic algorithms,” APA, 2017.

[10] C. Coronel and S. Morris, “DATABASE SYSTEMS,” 2017. [Online]. Available: www.cengage.com/highered

BIOGRAPHY

Sugiyatno has published some papers about Network and Security. She is now a lecturer of Informatics department in Universitas Bhayangkara Jakarta Raya.