IMPLEMENTATION OF THE RIJNDAEL ALGORITHM ON WEB-BASED WHISTLEBLOWING SYSTEM

Abdul Latif[1]*; Ai Ilah Warnilah[2]; Siti Khotimatul Wildah[3]

Sistem Informasi Kampus Kota Pontianak[1]
Universitas Bina Sarana Informatika
www.bsi.ac.id
abdul.bll@bsi.ac.id*

Sistem Informasi Kampus Kota Tasikmalaya[2]
Universitas Bina Sarana Informatika
www.bsi.ac.id
ai.aiw@bsi.ac.id

Teknologi Komputer[3]
Universitas Bina Sarana Informatika
www.bsi.ac.id
siti.ska@bsi.ac.id

Abstract— *In carrying out its responsibilities, an employee works for an agency or company and also works with his colleagues, whether they are co-workers or their own superiors. So it is very important for an employee to gain trust in his work environment. If there is a violation or behavior that deviates from an employee in the work environment, then there must be someone who reports it but of course by protecting the identity of the reporter. Based on these problems, the authors make and design a web-based whistle blowing application to protect the identity of people who report violations that occur in their work environment. This whistle blowing web is created using cryptographic algorithm methods. Cryptographic algorithms work by disguising data or information into a form of password that has no meaning. The author uses the Rijndael algorithm to encrypt the complainant's data. So that by using the Rijndael algorithm on this web-based Whistleblowing system, the data or reporting information will be safe in the database and it is hoped that an optimal system will be created for data and information security.*

Keywords: *Whistleblowing System, Cryptographic Algorithm Method, Web Engineering, Rijndael.*

Intisari— *Dalam melaksanakan tanggung jawabnya, seorang karyawan bekerja kepada sebuah instansi atau perusahaan dan juga bekerja dengan rekannya, baik itu rekan kerja maupun atasannya sendiri. Maka sangat penting bagi seorang karyawan untuk mendapatkan kepercayaan di lingkungan kerjanya. Apabila terjadi pelanggaran atau perilaku yang menyimpang dari seorang karyawan di lingkungan kerja, maka harus ada yang melaporkan hal tersebut namun tentunya dengan melindungi identitas pelapor itu. Berdasarkan permasalahan tersebut, penulis membuat dan merancang aplikasi whistleblowing berbasis web untuk melindungi identitas orang yang melaporkan pelanggaran yang terjadi dilingkungan kerjanya. Web whistleblowing ini dibuat dengan menggunakan metode algoritma kriptografi. Algoritma kriptografi bekerja dengan cara menyamarkan data atau informasi menjadi bentuk sandi yang tidak mempunyai makna. Penulis menggunakan algoritma Rijndael dalam mengenkripsi data pelapor. Sehingga, dengan menggunakan algoritma Rijndael dalam Whistleblowing sistem berbasis web ini, maka data pelapor atau informasi akan aman pada basis data dan diharapkan akan terciptanya sebuah sistem yang optimal untuk pengamanan data dan informasi.*

Kata Kunci: *Whistleblowing System, Metode Algoritma Kriptografi, Web Engineering, Rijndael.*

Vol. 19, No. 2 September 2022 | DOI https://doi.org/10.33480/techno.v19i2.3861

INTRODUCTION

In carrying out his responsibilities, an employee does not only work for the benefit of the company or agency, but also for the benefit of other parties, be it superiors, colleagues, or other parties. Sometimes, employees in the company, superiors, or the company itself do not carry out their responsibilities properly.

One way to reveal violations or deviant behavior committed by employees, superiors, or the company itself is by whistleblowing. Whistleblowing is a complex process involving personal and organizational factors. According to Komite Nasional Kebijakan Governance (KNKG) or National Committee on Governance Policy in Yusar Sagara's research (Sagara, 2018), whistleblowing is the disclosure of violations or unlawful, unethical/immoral acts or other actions that can harm the organization or stakeholders, which are carried out by employees or organizational leaders to the leadership of the organization or other institutions that can take action for the violation. Meanwhile, someone who does whistleblowing is called a whistleblower. Every employee who reports a violation of deviant behavior by other employees, superiors, or even the company, does not want their identity to be known by anyone. When an employee becomes aware of a fraud, he or she can report the fraud to his employer when he is confident that his employer can eradicate the fraud (Tyas & Utami, 2020). To maintain the confidentiality of the data or the identity of the reporter, a cryptographic algorithm is needed.

Cryptography is the study of mathematical methods related to information security aspects, including data confidentiality, data validity, data integrity, and data authentication (Santoso, 2021).

According to Fadma et al, there are 3 main criteria of cryptography which are also aspects of information security, including: confidentiality, data integrity, and authentication (Abella et al., 2022).

The cryptographic algorithm that will be used to solve the problem of identity security in a web-based whistleblowing system is using the Rijndael cryptography method.

The Rijndael or known as AES (Advanced Encryption Standard) is a cryptographic algorithm was designed by Vincent Rijmen and John Daemen from Belgium (Rizal et al., 2019). This algorithm came out as the winner in the cryptographic algorithm contest held by the United States government's NIST (National Institutes of Standards and Technology) on November 26, 2001. Rijndael's algorithm is known as the Advance Encryption Standard (AES) (Smid, 2021).

This algorithm can be used to secure the reporting data in the database. With this algorithm, it is hoped that an optimal system will be created for securing data or the identity of the reporter and the information contained in the database.

By implementing the Rijndael algorithm cryptographic technique, the system can secure the identity of the reporter stored in the database. As well as being able to create an optimal system for securing the identity of the reporter and providing a sense of security to the reporter in reporting irregularities that occur.

Some of the literature related to the use of the Rijndael algorithm include research conducted by Fathurrahmad and Ester from AMIK Indonesia (Fathurrahmad & Ester, 2020) with the title "Development And Implementation Of The Rijndael Algorithm And Base-64 Advanced Encryption Standard (AES) For Website Data Security". The research goals included the development of Base64 and the algorithm modified by Rijndael. Integrating the Base64 and AES Rijndael algorithms into the proposed algorithm is known to result in greater data security, according to research done through the encryption and decryption process. If the efficiency indicates that the proposed algorithm can be used as an alternative to the Base64 algorithm. In implementation, the speed of the proposed algorithm is good, but this can be seen from the encryption process and description, and the resulting bits are not significantly affected.

Furthermore, research conducted by Rinmar Siringoringo (Siringoringo, 2020) entitled "Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File" shows that the use of cryptographic algorithms can secure file. This study aims to build a file security application using the Rijndael algorithm and RSA cryptography. As a result, the system built is capable of encrypting and decrypting selected files with a 128-bit algorithm key length. The results of this study obtained encryption and decryption systems for plaintext and symmetric keys (sessionkey) with a combination of the Rijndael and RSA algorithms. The result of plaintext encryption on the built system is in the form of a character code, while for session key encryption it is in the form of a number code.

Research conducted by Setevi Liana Setiadi (Setiadi, 2019) entitled Perancangan Keamanan Data menggunakan Rijndael 256 pada Sistem Pusat Data Klasis Gunung Kidul Berbasis Client Server aims to design security in the data center system, especially on congregation data and offering data on the website of GKJ (Gereja Kristen Jawa). The author uses the Rijndael algorithm in his research, because according to him, this algorithm is an algorithm that has a very good operating speed. The security system application was built using the Rijndael 256 algorithm which was applied to secure

congregational data and GKJ Klasis Gunung Kidul offering data and was very helpful in securing very important data, so that only certain people could access the data. Data can be stored on the database server in the form of ciphertext and can be displayed again through the decryption process in plaintext (original text).

Research conducted by Rizal (Rizal et al., 2019) entitled "Cryptographic Symmetry Analysis with AES Algorithm for Safeguarding Data at Government Agencies". This research produce a program that can encrypt and decrypt data using the AES algorithm to secure data at Government Agencies. AES algorithm has been successfully applied to encrypt files with various extensions such as .doc, .xls, .ppt, .pdf, .jpg, .png. .MP4 and .Mp3, and the plain text can be recovered just like the original file. Data protected by the AES encryption method will not be corrupted provided it does not include text addition or deletion, trimming, brightness addition, and other edits that may alter the encrypted data.

Furthermore, in Aditya Ahmad Pradypta research (Pradypta, 2022) entitled "Perancangan Aplikasi Data Security Dalam Melindungi Informasi Digital Menggunakan Teknik Algoritma Rijndael Berbasis Desktop", examines desktop-based digital information security to secure important data such as files with extensions doc, exe, mp3, swf, mp4 , avi and others. the application of the rijndael algorithm to various file formats can be encrypted properly with the extension format (*.encrypt), and can be decrypted back into the previous format..

Then in a previous study entitled "Penerapan Ilmu Kriptografi Dalam Mengamankan Suastu File Citra Digital Dengan Menggunakan Algoritma Base64 Dan Rijendel" by Abdul Haris (Haris, 2020). In this study, the author wants to apply the algorithm contained in cryptography to secure the image when it is stored or when it wants to be sent so that no information leaks occur and the confidentiality of the information in the image is maintained. This study shows that if image data is used in encryption with the Bas64 algorithm, it will produce a temporary cipher or cipher which will then be re-encrypted with the Rijendel algorithm (AES). The process of extracting or decrypting the image can be done using the Rijendel (AES) algorithm first, so that it produces a pre-chiper and continues decrypting with the Base64 algorithm, so that it produces an initial plain image. The encryption and decryption system in this study uses two algorithms, which use a double-encryption and double-decryption system which goes through two processes.

Then in a study entitled "Column Level Database Encryption Using the Rijndael Algorithm and Dynamic Keys in Learning Management Systems" by Mursalat (Mursalat et al., 2022), which aims to see the possibility of a successful key guessing attack on the Learning Management System (LMS) database. By using the proposed method, it appears that the probability of success of the key guessing attack is smaller than using the previous method proposed by Francis Onodueze. The key used to encrypt passwords with the Rijndael method is a static key so that key guessing attacks can be carried out easily using the brute force method. To improve security against key guessing attacks, a dynamic key generation method is proposed using HMAC-DRBG. Based on the results of the performance and safety evaluation of the previously proposed and currently proposed methods, it can be concluded that the time complexity for running the two methods is the same.

In a study entitled "Implementation of a File Encryption Software 'Hyde' using RIJNDAEL Algorithm (AES)", Itunuoluwa Isewon (Isewon, 2022) explains that the research aims to provide solutions to data security problems. , in which case an unauthorized user or attacker is the case. , have access to their data and information during transmission across different platforms. In addition, users want to embed messages in files such as image shorthand and text ciphers. problem. The Hyde System is a tool that provides data integrity services for important or private files and documents. This provides an extra layer of security for sensitive documents. If the security of a computer system is breached, either physically or remotely, sophisticatedly encrypted files or texts prevent unauthorized access, thereby preventing further attacks. The future scope of this idea is to develop cryptographic tools that are integrated as a component or service in a computer operating system to provide a seamless user experience that allows users to easily take advantage of the service. service. Future development will work to provide a service that embeds options in the file object's context menu for plain text/file encryption or encrypted file decryption.

MATERIALS AND METHODS

A. Research Methods

Research methods and data collection techniques used in this study, including Observation, Interview, Literature Review, and Development Method using waterfall model.

In this research, the waterfall method is adopted as the development method by Rosa A.S and Shalahudin (A.s. & Shalahuddin, 2016). The stages of the waterfall model are described as follows:

Vol. 19, No. 2 September 2022 | DOI https://doi.org/10.33480/techno.v19i2.3861

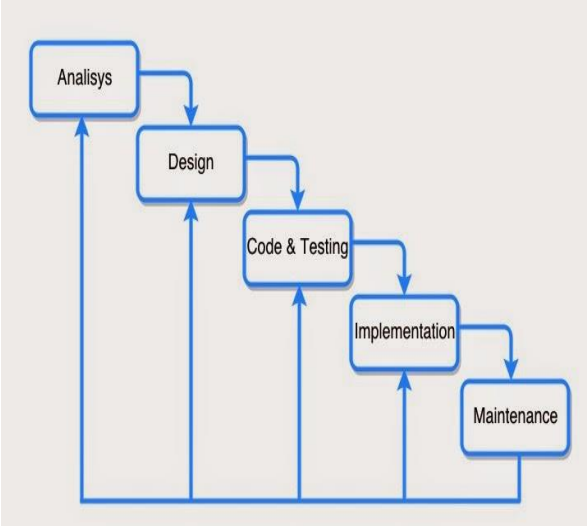

Figure 1. Waterfall Model

At the Analysis stage, the author collects all requirements related to hardware, software, user requirements, and system requirements. Then at the system design stage, the authors design diagrams, such as entity relationship diagrams (ERD) and Logical Relational Structure (LRS) diagrams. Furthermore, at the coding and testing stage, testing is carried out with blackbox testing which includes input and output processes, login form testing, form validation, and so on. At the implementation stage, the author uses a server that is hosted on a hosting provider and tested as a whole. Finally, at the maintenance stage, regular data backups are carried out. at this stage it is also possible to repeat the development process from specification analysis to changes to existing software, but not to create new systems.

The data source for this study is primary data from the data sources such as books and magazine articles. Methods of data collection are through observations, interviews, and literature searches. The data analysis used was qualitative.

B. Rijndael Algorithm

AES Rijndael Algorithm recognizes 128-bit plain text and generates 128-bit length decrypted text using a secret key check using 128, 192, or 256 bits. It is an alternative permutation network design with a unique set of steps named rings (Pasuluri, 2021). A certain number of executions depends on the length of the AES algorithm key when implementing the algorithm.

Key length and block size can be selected independently. The flowchart below is the flow of data encryption using the Rijndael Algorithm:

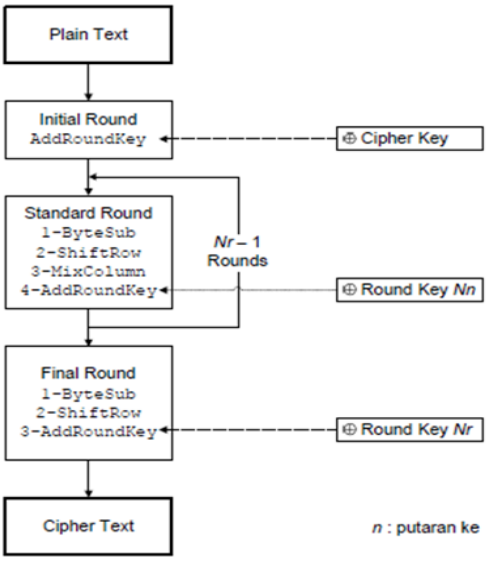

Figure 2. Rijndael Encryption Process Flowchart

Broadly speaking, AES encryption is described as follows. The input is an original 128-bit script, while the output is a random 128-bit script. Each transformation is performed directly on the script, starting with the AddRoundKey(0) transformation. So every transformation must have an inverse so that the random script can be decrypted. In rounds 1 to Nr − 1, SubBytes, ShiftRows, MixColumns and AddRoundKey transformations are performed on the text. In the last round (Nr), the SubBytes, ShiftRows and AddRoundKey transformations are performed on the script (MixColumns transformation is not performed). In total there are Nr rounds. The number of turns (Nr) depends on the size of the key used.

RESULTS AND DISCUSSION

In creating a whistleblowing website that is integrated with the Rijndael algorithm, the authors analyze several needs such as hardware, software, user needs, system requirements, and system design.

In Waterfall Model, the discussion and research results are as follows:

A. Requirement Gathering and Analysis

At this stage, the author collects all requirements related to hardware, software, user requirements, and system requirements. The author uses a Dell Server with a multi-core Intel® Xeon® Silver 4214 CPU 2.20GHz with 5GB RAM and 500GB SSD for hardware and software needs. Meanwhile, the operating system used is CloudLinux for the server.

Then for user needs, using a computer with an Intel Dual-core 2.0 Ghz Processor, 2 GB DDR2 RAM Memory, 250 GB Harddisk Memory, mouse, keyboard, monitor with a minimum screen resolution of 1024 x 768, as well as an internet connection with a minimum speed of 20 Mbps

Then for user needs, this website consists of 2 access rights, namely admin and user. Where, the user is the reporter, and the admin only has the right to verify the data without being able to change and see the identity of the reporter. For system requirements, the author uses MySQL for the database and PHP 7 for website creation, as well as the mcrypt module (MCRYPT_ENCRYPT and MCRYPT DECRYPT) of type MCRYPT_RIJNDAEL_256 with Electronic Code Book (ECB) mode.

B. System Design

At the system design stage, the authors design diagrams, such as entity relationship diagrams (ERD), Logical Relational Structure (LRS) diagrams, and navigation structure.

In system design which aims to find out the functions that can be performed from the system created, including:

- ERD

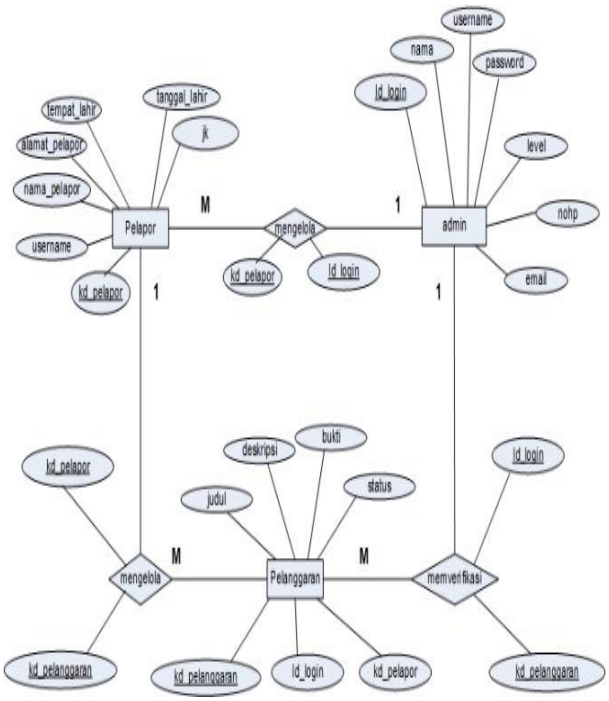

Figure 2. ERD Whistleblowing web-based Application

Figure 2 shows the relationship between the data store in the data relationship in this web-based whistleblowing application. In this application, there are 3 tables, namely admin, pelapor, and pelanggaran. The relationship between tables or entities in the development of this whistleblowing web-based is described in Figure 2.

- LRS

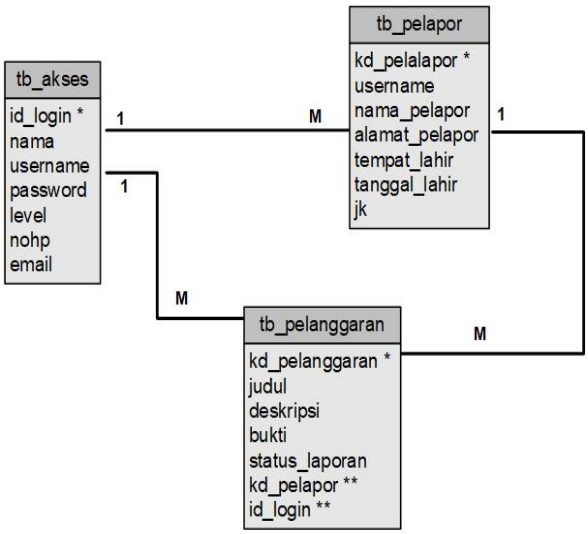

Figure 3. LRS Database

In Figure 3, the depiction of the diagram using the ERD transformation is presented in the form of LRS.

- Navigation Structure

A navigation structure describes how the various pages of your website are organized and connected to each other.

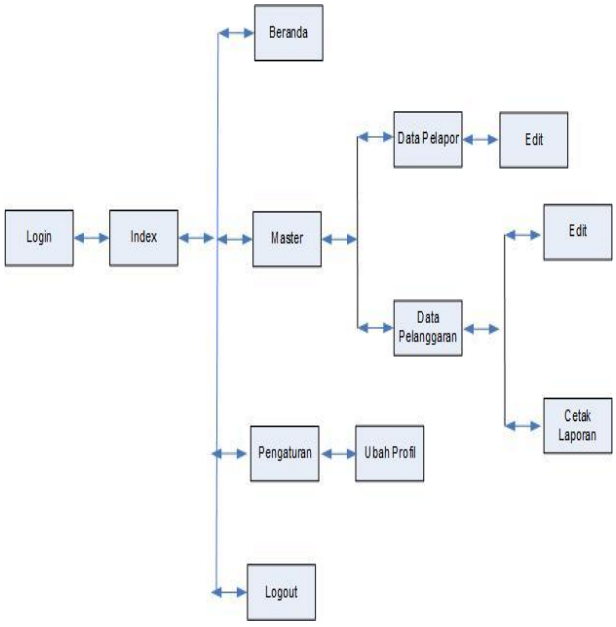

Figure 4. Admin Page Navigation Structure

Techno Nusa Mandiri: Journal of Computing and Information Technology
Vol. 19, No. 2 September 2022 | DOI https://doi.org/10.33480/techno.v19i2.3861

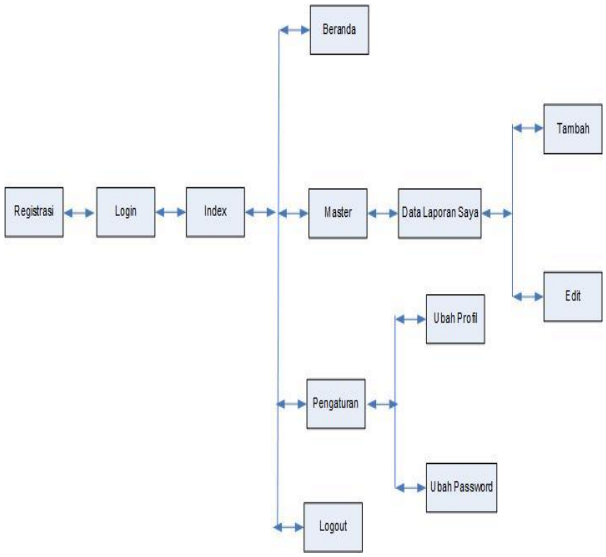

Figure 5. User Page Navigation Structure

C. Coding, Testing, and Implementation

Application development is done through program coding activities. PHP 7.0 was used as the programming language and MySQL 5.0 as the database during the development of this whistleblowing web-based application. Designing with the AdminLTE template.

Testing is carried out with blackbox testing which includes input and output processes, login form testing, form validation, and so on.

The results of the development and implementation of this web-based application are as follows:

1. Register Page

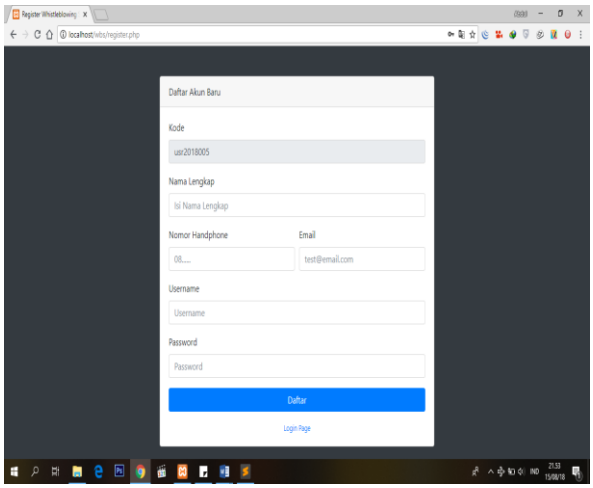

Figure 6. Register Page

This page is a page for users / complainants to create a new account to make a violation report.

2. Login Page

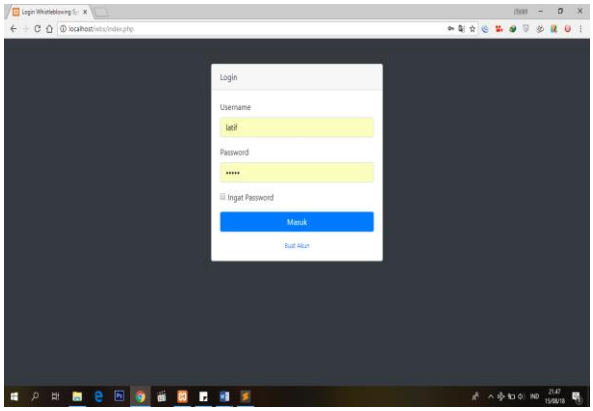

Figure 7. Login Page

After registering, users can login to the dashboard using the username and password that has been created.

3. Dashboard Admin

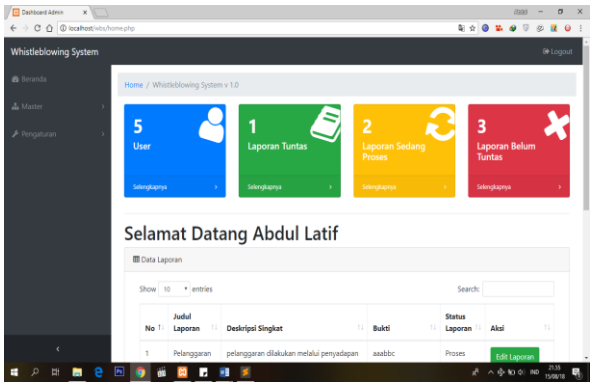

Figure 8. Admin Dashboard

This page contains all information including the number of users, a list of the number of reports, both completed and still in process.

4. Violation/Complaint Page

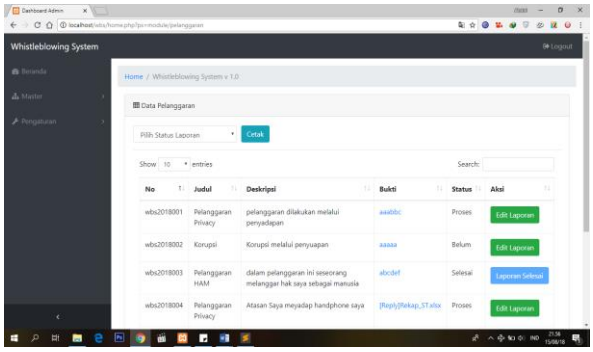

Figure 9. Complaint Page

This page will display all data on violations reported by the complainant, admins can verify report data, edit report status only, and print reports both based on status and all reports.

5. Profile Setting Page

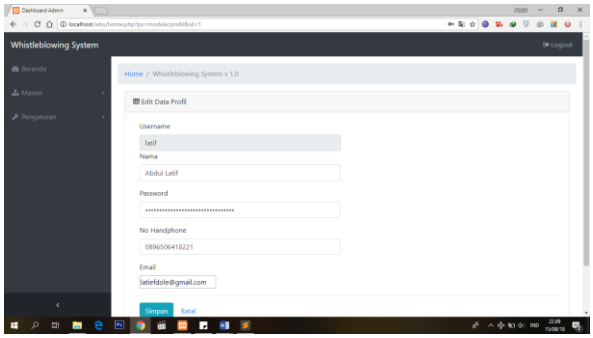

Figure 10. Profile Setting Page

On this page, users and admins can change their profile data.

6. Violation/Complaint Data Input Page

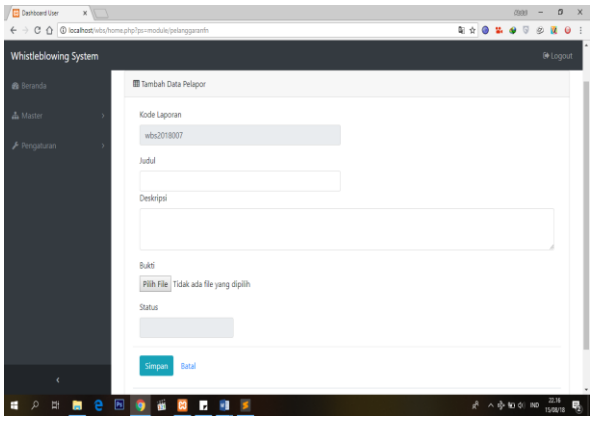

Figure 11. Complaint Data Input Page

On this page, users / reporters can report violations that occur without being able to identify them.

D. Maintenance

The Whistleblowing web-based application can be accessed via a web browser and run on a variety of operating systems. System maintenance is done through regular database backups, resource control by CPanel hosting, and system upgrades in case of system changes.

CONCLUSION

Based on the creation of an information system that implements the Rijndael algorithm on a website-based Whistleblowing system and various previous explanations above, it can be concluded that the Rijndael algorithm can be used to secure databases on a website-based whistleblowing system. So if a hacker manages to dump all or part of the tables from this whistleblowing application database, important data has been encrypted using AES-256. To decrypt it requires a special key. In addition, each reporter no longer has to worry about the threat of leakage of his personal data, so he can remain anonymous and this can also be a witness protection program. This system can also make it easier for the audit team of a government agency or company to manage audit reports. The weakness in this system is that when encrypting data, this application still uses a constant decryption key and can only be changed from the source code. For further development, the decryption key can use a variable that can change. So that each user has their own encryption key. It also doesn't have a feature to encrypt files yet. Hopefully, the evidence file can also be encrypted. Another drawback is that the mcrypt module in PHP only has support for PHP version 7.2 and no longer supports the latest PHP versions.

REFERENCE

A.s., R., & Shalahuddin, M. (2016). *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek*.

Abella, F. A., Ghiffari, M. B., Johana, M., & Simanjuntak, S. (2022). IMPLEMENTATION OF CRYPTOGRAPHY USING AES-128 ALGORITHM. *Jurnal Ilmu Komputer (JIKOMP)*, *1*(Maret), 9–13.

Dewi, R. R. K., Kartasurya, M. I., & Mawarni, A. (2017). Analisis Kebijakan Donor Darah Dan Implementasi Program Rekrutmen Donor Di Unit Donor Darah (UDD PMI) Kota Pontianak. *Jurnal Manajemen Kesehatan Indonesia*, *4*(2). https://doi.org/10.14710/jmki.4.2.2016.109-117

Fathurrahmad, & Ester. (2020). Development and Implementation of The Rijndael Algorithm and Base-64 Advanced Encryption Standard (AES) for Website Data Security. *International Journal of Computer Applications*, *9*(11), 9–12.

Haris, A. (2020). Penerapan Ilmu Kriptografi Dalam Mengamankan Suastu File Citra Digital Dengan Menggunakan Algoritma Base64 Dan Rijendel. *KOMIK (Konferensi Nasional Teknologi Informasi Dan Komputer)*, *4*(1), 215–222. https://doi.org/10.30865/komik.v4i1.2683

Isewon, I. (2022). Implementation of a File Encryption Software " Hyde " using RIJNDAEL Algorithm (AES). *International Journal of Computer Science and Information Security (IJCSIS)*, *20*(April). https://doi.org/10.5281/zenodo.7129308

Mursalat, A. S., Barmawi, A. M., & Yunanto, P. E. (2022). Column-Level Database Encryption Using Rijndael Algorithm and Dynamic Key on

Learning Management System. *Indonesia Journal of Computing*, *7*(April), 15–30. https://doi.org/10.34818/indojc.2022.7.1.609

Pasuluri, B. S. (2021). APPLICATION OF UT MULTIPLIER IN AES ALGORITHM AND ANALYSIS OF ITS PERFORMANCE. *IT in Industry*, *9*(3), 647–652.

Pradypta, A. A. (2022). Perancangan Aplikasi Data Security Dalam Melindungi Informasi Digital Menggunakan Teknik Algoritma Rijndael Berbasis Desktop. *Jurnal Maklumatika*, *9*(1), 68–76. https://maklumatika.i-tech.ac.id/index.php/maklumatika/article/view/141%0Ahttps://maklumatika.i-tech.ac.id/index.php/maklumatika/article/download/141/138

Rizal, M., Zamzami, E. M., & Zarlis, M. (2019). Cryptographic Symmetry Analysis with AES Algorithm for Safeguarding Data at Government Agencies. *International Journal of Information System & Technology*, *3*(1), 131–139.

Sagara, Y. (2018). Profesionalisme Internal Auditor Dan Intensi Melakukan Whistleblowing. *Liquidity*, *2*(1). https://doi.org/10.32546/lq.v2i1.127

Santoso, Y. S. (2021). Message Security Using a Combination of Hill Cipher and RSA Algorithms. *Jurnal Matematika Dan Ilmu Pengetahuan Alam LLDikti Wilayah 1 (JUMPA)*, *1*(1), 20–28. https://doi.org/10.54076/jumpa.v1i1.38

Setiadi, S. L. (2019). *Perancangan Keamanan Data menggunakan Rijndael 256 pada Sistem Pusat Data Klasis Gunung Kidul Berbasis Client Server*.

Siringoringo, R. (2020). Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File 31 Oleh : Rinmar Siringoringo Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File ARTICLE INFORMATION A B S T R A K. *Jurnal Optimasi Sistem Industri*, *02*(01), 31–42.

Smid, M. E. (2021). Development of the advanced encryption standard. *Journal of Research of the National Institute of Standards and Technology*, *126*. https://doi.org/10.6028/JRES.126.024

Tyas, E. Y., & Utami, I. (2020). Trust in leadership and incentives: Experimental study of whistleblowing intention. *Jurnal Akuntansi & Auditing Indonesia*, *24*(1), 43–54. https://doi.org/10.20885/jaai.vol24.iss1.art5