Design of Whistleblowing System in Higher Education Environment Based on Web Service

Natasha Diva Muljono[1], Ridwan Sanjaya[2], T. Brenda Chandrawati[3]
[1,2,3] Information Systems Department, Faculty of Computer Science
Soegijapranata Catholic University, Indonesia
[1]natashad.m48@gmail.com
[2]ridwan@unika.ac.id
[3]brenda@unika.ac.id

Abstract— Higher education faces various fraud challenges in the field of integrity. Whistleblowing is an important solution to reveal violations that occur in higher education. Whistleblowers often face a moral dilemma: reporting fraud or protecting the whistleblower. Support and protection for whistleblowers are important so that they feel safe and avoid unfair retaliation. To solve this problem, it is necessary to develop a web-service-based whistleblowing system that can be adapted to other universities. This system protects the privacy of the whistleblower by not asking for the whistleblower's data (anonymous) but using a unique code to track the progress of the report handling. Encryption of the code and report description using AES (Advanced Encryption Standard) increases the security of the report information so that only the authorized task force can access the information. Dashboard security is strengthened with a token to access the API that leads to the dashboard. At the same time, the distribution of reports based on the level of handling accelerates and ensures reliable handling of cases by the authorized task force.

Keywords— fraud, whistleblowing, whistleblowing system, anonymus, web service.

I. INTRODUCTION

Higher education faces the challenge of fraud in various areas of integrity, such as academics, ethics, and finance. Fraud is an unethical act that is intentionally committed for a specific purpose, such as deceiving or misleading other parties [1]. The main factors associated with fraud are motive or pressure, opportunity, and rationalization, known as the fraud triangle [2].

Only a few people dare to report when fraud occurs in an organization. Whistleblowing is an effort to reveal organizational violations driven by moral intentions to prevent harm to the organization [3]. Factors influencing whistleblowing include the whistleblower, the complaint about the offence, and the recipient of the report [4]. In science, the Retraction Watch website demonstrates the important role of whistleblowers in exposing data falsification and scientific fraud, which is quite well-known [5]. Whistleblowers are often faced with a moral dilemma between reporting fraud or protecting the individuals involved, so their protection is crucial [6].

To overcome these problems, developing a whistleblowing system in higher education is necessary to report anonymously and effectively. This system can influence fraudsters to reconsider their actions [6]. The system's effectiveness depends on factors affecting the whistleblower's decision to report the violation and the organization's response to potential reprisals against the whistleblower [2]. The system guarantees anonymity in reporting, allowing stakeholders to report violations without fear of repression. The process starts from anonymous reporting, grouping by scope, to handling the report by

an authorized task force with necessary actions, including policy changes or sanctions.

This system can be customized by each educational institution through the implementation of a web-service-based whistleblowing system that utilizes communication standards such as XML/JSON, SOAP, WSDL, and UDDI [7]. Web services allow reuse of the same logic across multiple applications, including desktop, mobile, and web [8], and have advantages in interoperability, platform independence, scalability, security, and integration with third-party systems [9]. The data exchange process has three web service components: Service Provider, Service requestor, and Service Registry [10].

RESTful web services are parts of back-end applications that are accessed by front-end applications with specific security methods [11]. REST (Representational State Transfer) is a web service architecture tool that focuses on transferring and requesting data using HTTP. REST recognizes URIs and converts them using POST, DELETE, PUT, and GET commands in JSON data format [12].

Each college can develop front-end applications using web services architecture and access the back-end functions needed for the whistleblowing system. Thus, this approach helps higher education institutions provide a standardized whistleblowing system and facilitates extensive development.

II. METHOD

This research uses a system development method known as Rapid Application Development (RAD), one of the System Development Life Cycle (SDLC) models. RAD is a software development model that emphasizes a concise development cycle. The RAD method can be a basis for developing better systems with speed, accuracy, and lower costs. The RAD system development method is chosen because it has various advantages, such as a shorter development cycle, greater flexibility, increased user involvement, and minimizing errors [13]. The stages in the RAD method can be seen in Figure 1.

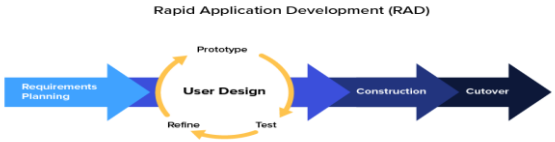

Figure 1. Stages of the RAD Method
Source : https://bitlabs.id/blog/wp content/uploads/2021/01/tahapan-rad.png

III. RESULTS AND DISCUSSION

A. RESULT

1. ERD Whistleblowing System

Entity Relationship Diagram (ERD) is created to provide an overview of the interrelationship of entities in the database. One-to-one, one-to-many, and many-to-many are three types of relationships between entities [14]. The ERD of the Whistleblowing System can be seen in Figure 2.

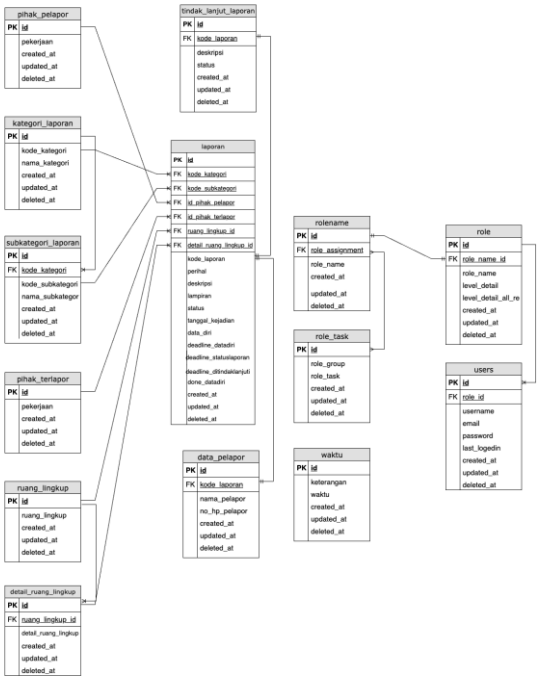

Figure 2. ERD of Whistleblowing System

2. Flowchart Whistleblowing System

The flowchart is a visual representation or diagram that uses graphical symbols to

describe the sequence of steps in a process or workflow in the system [15].

The Whistleblowing System process flow from the Whistleblower side is depicted in Figure 3. Users who act as whistleblowers can make reports related to violations by filling out the forms that have been provided. After completing the report form, the reporter will be given a unique code to track the report's status.

The reporter can enter the unique code into the system to track the report's progress. In following up on the report, the task force requires the reporter's data to be asked for further information about the report. In that case, the reporter is given the choice of whether they are willing. The report will be followed up if the reporter can fill in personal data information. However, if the reporter is unwilling to provide personal data information, the report handling will not continue.

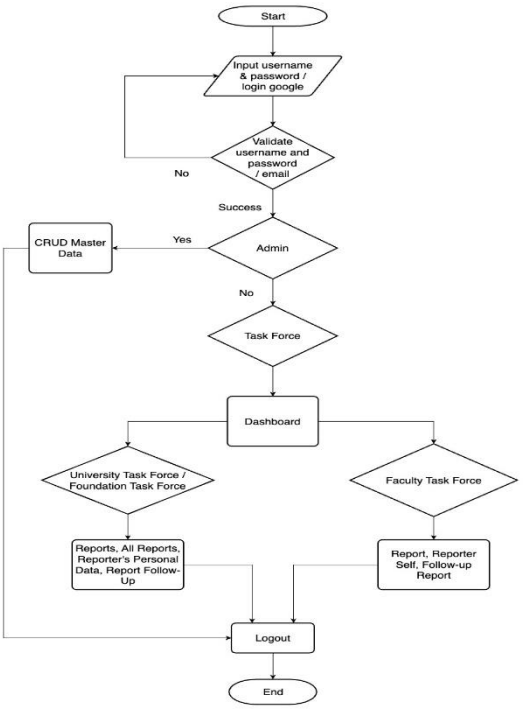

Figure 3. Flowchart of Whistleblowing System on the Whistleblower Side

Figure 4 explains the process flow on the Whistleblowing System Dashboard for admin and task force. The process begins with login, where users enter credentials such as username and password or use login via Google, which the system verifies. Based on identification from the system, users will be directed to the appropriate menu.

If the user is identified as an Admin, then the user has CRUD access to manage master data.

If the user is identified as Faculty Task Force, University Task Force, and Foundation Task Force, then the user can handle reports with different levels of responsibility. The University Task Force and Foundation Task Force have special rights to view all reports under their handling scope.

The last process in this system is logout, where users exit the session that is being used.

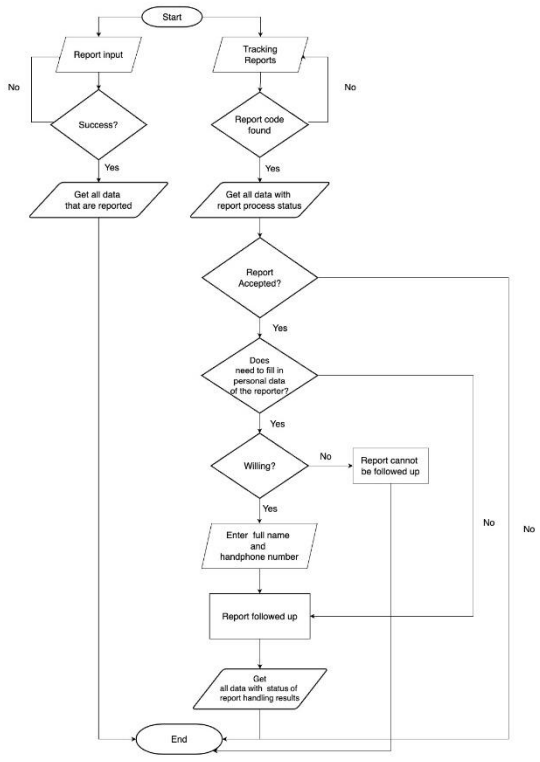

Figure 4. Flowchart of Whistleblowing System on the Admin and Task Force Side

The concept applied in developing this whistleblowing system is the use of web services. This system allows interaction and data exchange between various applications

or systems via the Internet network. The web service concept facilitates efficient communication and information exchange between different systems without being constrained by differences in programming languages.

Figure 5 shows the communication model between the client, web server, and database in the Whistleblowing System. The process starts when the client sends an HTTP request to the server, either "POST" to send data or "GET" to retrieve data. The web server receives the request, determines the action, and sends the appropriate query to the database if it requires data from the database. The database executes the CRUD query and returns the results to the server.

The server processes the results from the database, displays them in JSON format, and sends them back to the client. The client receives this response and can display, process, or perform other actions based on the data.

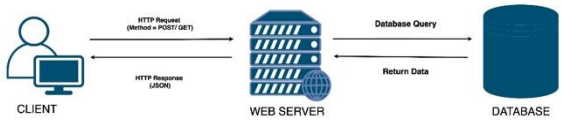

Figure 5. RESTful API Communication

The initial view of the Whistleblower System in Figure 6 provides information on the function, purpose, and instructions on how to use the platform.

Figure 6. Reporter Side Initial View

Figure 7 displays the report form. At this stage, the reporter can report violations throughout the university.

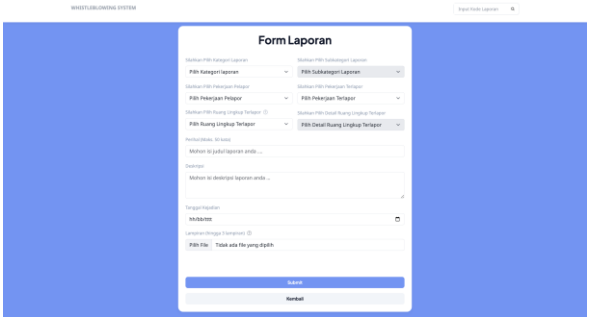

Figure 7. Display of the Report Form

After successful report input, the reporter will be redirected to a page containing report information and a unique code, as shown in Figure 8. This unique code allows tracking of report status and information related to handling until completion.

Figure 8. Display after the report is successfully inputted

Figure 9 shows the report search view with the report's unique code in the search field. In this view, a progress bar contains the stage at which the report is processed. Stage 1 shows when the report is successfully inputted, and stage 2 contains information on whether the report is accepted or rejected. If the report is denied, the process stops at that stage.

If the report is accepted, there will be two criteria: the report is accepted without requiring the reporter's data, or the report is accepted, but the task force needs the reporter's data for report follow-up. If the report is accepted and the task force requires the reporter's data, the reporter will be given the option to be willing or not to fill in the personal data information. If the reporter is willing, the reporter's unique data form will be given, which must be filled in by the specified deadline; if the personal data has been filled in, the report will be

followed up. However, the report will not be followed up if the reporter is unwilling.

The third stage contains information from the follow-up of the report. There are three types of follow-up status of the report: proven but insignificant impact, proven with significant impact and not proven. For those proven, there are two follow-ups: the application of sanctions or policy changes.

The fourth stage is the final phase, presenting the reporting process's final information. If the report has been completed, this stage will contain information that the report has been completed. If the report is rejected, the information at this stage will indicate that the report has been rejected. If the report is declared expired because the reporter did not complete the personal data by the deadline, this stage will provide information that the report has expired.

Figure 9. Report Search Display

The initial stage the Admin and Task Force carry out to enter the system is logging in. At the login stage, users have two options to enter the system: a username and password or a Google login found on the application interface, as shown in Figure 10.

Figure 10: Admin and Task Force Login View

After a successful login, if the user is identified as the Task Force, then the user will be directed to the dashboard page, as shown in Figure 11. This page presents data summaries and graphs regarding the reports available based on specific criteria.

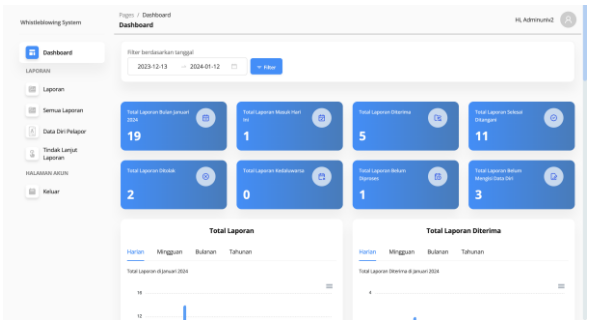

Figure 11. Task Force Dashboard View

Figure 12 displays the report menu for the task force to process reports. The task force has the option to accept or reject the report on the "action" button. When accepting, the task force can choose whether or not the reporter's data is required. If not, the report follow-up process can be done immediately; if necessary, the report follow-up can be done after the reporter fills in the reporter's personal data information. The level of report handling by the task force depends on the level of detail at login. The Faculty Task Force handles study programs under the faculty, the University Task Force handles faculties in the university, and the Foundation Task Force handles the university level.

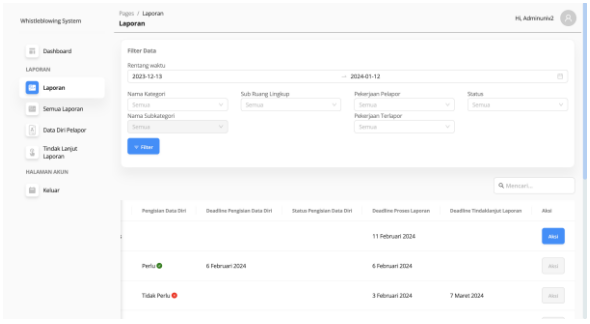

Figure 12. Display of the Report Menu

Figure 13 shows the appearance of the all reports menu; this menu can only be accessed if, at the time of login, the user is identified as the University Task Force and the Foundation Task Force. In this menu, the University Task Force can see reports that are under the scope of its handling; the University Task Force can see reports that

are within the scope of the faculty and study program, while the Foundation Task Force can see reports that are under the scope of its handling as well, namely the scope of the university, faculty and study program.

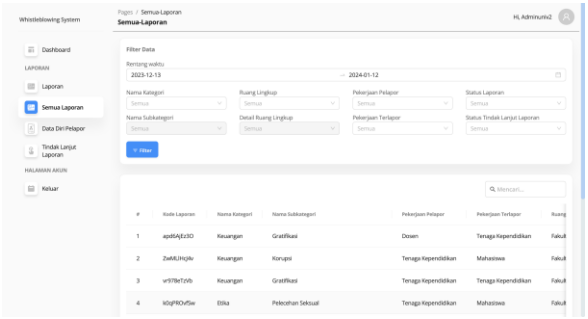

Figure 13. All Reports Menu Display

Figure 14 displays the reporter's data menu, which contains information about the reporter's data.

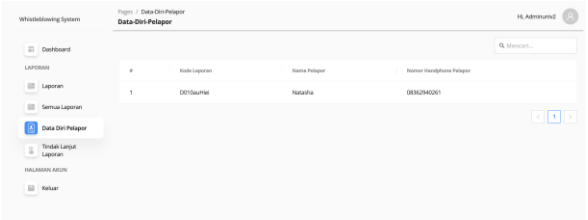

Figure 14. Display of the Reporter's Personal Data Menu

Figure 15 displays the report follow-up menu, where the task force can add follow-up to reports that have been received; reports that can be followed up are reports that meet the criteria, namely reports received without requiring the reporter's data. Second, reports received require the reporter's data, and the reporter has filled in the personal data.

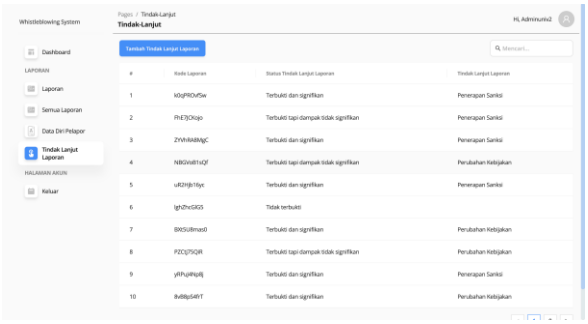

Figure 15. Display of the Report Follow-up Menu

The CRUD (Create, Read, Update, Delete) data operation process on the dashboard can only be accessed by users identified as admins. The admin crud menu display can be seen in Figure 16.

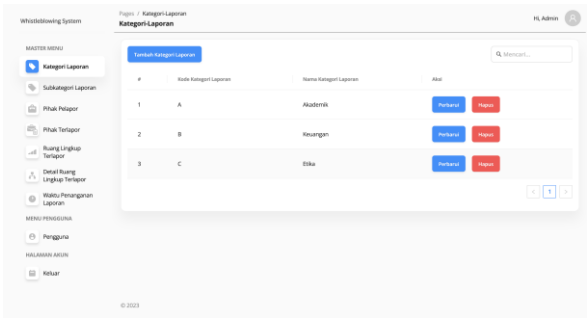

Figure 16. Admin CRUD Menu Display

B. DISCUSSION

System testing is done through Black box Testing. On the reporter side, the test results show that the system can operate properly in the process of inputting and tracking reports. On the task force side, it shows that the system can function properly, as seen from the task force's ability to access the dashboard, process reports, view the reporter's data, view all reports, and follow up on reports. Finally, on the admin side, testing shows that the system runs well, reflected in the admin's ability to perform the CRUD process on the master data.

IV. CONCLUSION

The Whistleblowing System emphasizes legal protection through anonymous reporting or without asking for the reporter's data but using a unique code to track the progress of handling the report. The system is strong in security with token for access to each API (Application Programming Interface) in the web service that leads to the dashboard. For report security, the report code and description are encrypted using AES (Advanced Encryption Standard), so only the authorized task force can view the information. Then this system uses the concept of web services so that APIs are available to generate data summaries that can be represented on the dashboard.

Finally, the distribution of reports based on the level of handling accelerates and ensures reliable handling of cases by the authorized task force.

REFERENCES

[1] W. Yulian Maulida and B. Indah Bayunitri, "The influence of whistleblowing system toward fraud prevention," *Int. J. Financ. Accounting, Manag.*, vol. 2, no. 4, pp. 275–294, 2021, doi: 10.35912/ijfam.v2i4.177.

[2] D. Puryati and S. Febriani, "The Consequence of Whistleblowing System and Internal Control toward Fraud Prevention: A Study on Indonesian State Owned Enterprise," *Int. J. Bus. Technol. Manag.*, vol. 2, no. 3, pp. 35–48, 2020.

[3] K. A. Kurniawan Saputra, B. Subroto, A. F. Rahman, and E. Saraswati, "Issues of morality and whistleblowing in short prevention accounting," *Int. J. Innov. Creat. Chang.*, vol. 12, no. 3, pp. 77–88, 2020.

[4] A. N. S. Hapsari and D. W. Seta, "Identifikasi Kecurangan Dan Whistleblowing Universitas," *J. Ris. Akunt. dan Keuang.*, vol. 7, no. 1, pp. 131–144, 2019, doi: 10.17509/jrak.v7i1.15424.

[5] F. Anvari, M. Wenzel, L. Woodyatt, and S. A. Haslam, "The social psychology of whistleblowing: An integrated model," *Organ. Psychol. Rev.*, vol. 9, no. 1, pp. 41–67, 2019, doi: 10.1177/2041386619849085.

[6] S. Wahyudi, T. Achmad, and I. D. Pamungkas, "Whistljeblowing system and fraud early warning system on village fund fraud: The Indonesian experience," *Int. J. Financ. Res.*, vol. 10, no. 6, pp. 211–217, 2019, doi: 10.5430/ijfr.v10n6p211.

[7] P. R. Harihara Subramanian, *Hands-On RESTful API Design Patterns and Best Practices: Design, develop, and deploy highly adaptable, scalable, and secure RESTful web APIs*. Packt Publishing Ltd, 2019.

[8] E. N. Hamdana and Meyti Eka Apriyani, "Analisis Implementasi Restfull Web Service Menggunakan Resource-Oriented Architecture," *J. Inform. Polinema*, vol. 6, no. 2, pp. 57–60, 2020, doi: 10.33795/jip.v6i2.335.

[9] N. Yellavula, *Hands-On RESTful Web Services with Go*, Second Edi. Second Edi.Birmingham: Packt Publishing Ltd, 2020.

[10] S. Priadi, "Implementasi Rest Dalam Membangun Web Service Menggunakan Golang (Studi Kasus: Aplikasi Satudikti)," 2022.

[11] S. I. Adam, J. H. Moedjahedy, and J. Maramis, "RESTful Web Service Implementation on Unklab Information System Using JSON Web Token (JWT)," *2020 2nd Int. Conf. Cybern. Intell. Syst. ICORIS 2020*, 2020, doi: 10.1109/ICORIS50180.2020.9320801.

[12] I. O. Suzanti, N. Fitriani, A. Jauhari, and A. Khozaimi, "REST API Implementation on Android Based Monitoring Application," *J. Phys. Conf. Ser.*, vol. 1569, no. 2, 2020, doi: 10.1088/1742-6596/1569/2/022088.

[13] E. Listiyan and E. R. Subhiyakto, "Rancang Bangun Sistem Inventory Gudang Menggunakan Metode Waterfall Studi Kasus Di Cv. Aqualux Duspha Abadi Kudus Jawa Tengah," *KONSTELASI Konvergensi*

Teknol. dan Sist. Inf., vol. 1, no. 1, pp. 74–82, 2021, doi: 10.24002/konstelasi.v1i1.4272.

[14] M. K. Dedy Rahman Prehanto, S.Kom., *BUKU AJAR KONSEP SISTEM INFORMASI*. Scopindo Media Pustaka, 2020.

[15] U. Rusmawan, *Teknik Penulisan Tugas Akhir dan Skripsi Pemrograman*. PT Elex Media Komputindo, 2019.

.