

CIPHERTEXT-POLICE ATTRIBUTE BASED ENCRYPTION UNTUK PENGADUAN TINDAK PIDANA KORUPSI

I Gede Totok Suryawan¹, I Putu Susila Handika²

¹Program Studi Teknik Informatika ^{1) 2)}

STMIK STIKOM Indonesia ^{1) 2)}

totok.suryawan@stiki-indonesia.ac.id ¹⁾ susilaandika@gmail.com ²⁾

ABSTRACT

This paper discusses the results of research on the implementation of the Ciphertext Police Attribute Based Encryption (CP-ABE) in the system of complaints of corruption. The study was conducted at Bali's High Prosecutors Office as one of the state institutions that has the task of preventing and eradicating corrupt acts. The Bali High Prosecutor's Office has facilitated the public to make corruption complaints through the legal service post and public complaints in the Bali High Prosecutors Office. In addition to legal service posts and public complaints, the Bali Attorney General's Office also facilitated the public to make corruption complaints through a website page. Noting these problems in this research, a corruption online complaint system has been developed which is equipped with data protection by implementing a CP-ABE encryption method. This CP-ABE implementation places an access policy on encrypted data, and a set of descriptive attributes resides in the user's private key. If the specified attribute meets the access policy, the user can describe the complaint data. With this scheme, the security of complaints data is maintained, where in each data an encrypted access policy has been placed, and a set of descriptive attributes is in the private key of the reporter. So that the complaint data (Ciphertext) can only be described by the recipient of the complaint if the set of recipient key attributes matches the ciphertext attribute. The developed system can encrypt with a number of attributes as an access policy, generate keys, send complaints, describe complaint data using keys. Evaluation results show the system can run well in accordance with the specified test scenario.

Keywords: Corruption Complaints System, Cryptograph, Ciphertext Police Attribute Based Encryption, CP-ABE.

ABSTRAK

Paper ini membahas tentang hasil penelitian tentang implementasi *Ciphertext Police Attribute Based Encryption* (CP-ABE) pada sistem pengaduan tindak pidana korupsi (tipikor). Penelitian dilakukan di Kejaksaan Tinggi Bali sebagai salah satu lembaga negara yang memiliki tugas dalam pencegahan dan pemberantasan tindak pidana korupsi. Kejaksaan Tinggi Bali telah memfasilitasi masyarakat untuk melakukan pengaduan tipikor melalui pos pelayanan hukum dan pengaduan masyarakat yang ada di Kantor Kejaksaan Tinggi Bali. Selain pos pelayanan hukum dan pengaduan masyarakat, Kejaksaan Tinggi Bali juga memfasilitasi masyarakat untuk melakukan pengaduan tipikor melalui halaman website. Dari observasi awal yang dilakukan bahwa fasilitas pengaduan di halaman website Kejati Bali belum lengkap karena hanya memfasilitasi masyarakat untuk memberikan data pelapor berupa nama, alamat, email dan data pengaduan berupa topik/judul aduan, keterangan aduan serta fasilitas keamanan berupa *captcha*. Pada form pengaduan ini tidak memiliki fitur tentang perlindungan privasi dan kerahasiaan data pengaduan. Memperhatikan permasalahan tersebut pada penelitian ini telah dikembangkan sistem pengaduan online tipikor yang dilengkapi dengan perlindungan data pengaduan dengan cara menerapkan salah satu metode enkripsi yaitu CP-ABE. Implementasi CP-ABE ini menempatkan kebijakan akses pada data yang dienkripsi, dan satu set atribut deskriptif berada di kunci pribadi pengguna. Jika atribut yang ditetapkan memenuhi kebijakan akses, pengguna dapat mendeskripsikan data pengaduan. Dengan skema ini keamanan data pengaduan menjadi terjaga, dimana pada setiap data telah ditempatkan kebijakan akses yang terenkripsi, dan satu set atribut

deskriptif berada di kunci pribadi pelapor. Sehingga data pengaduan (Ciphertext) hanya bisa dideskripsikan oleh penerima pengaduan jika himpunan atribut kunci penerima sesuai dengan atribut ciphertext. Sistem yang dikembangkan dapat melakukan enkripsi dengan sejumlah atribut sebagai kebijakan akses, menghasilkan kunci, mengirim pengaduan, mendeskripsikan data pengaduan menggunakan kunci. Hasil evaluasi menunjukkan sistem dapat berjalan dengan baik sesuai dengan skenario pengujian yang ditetapkan.

Kata Kunci : *Sistem Pengaduan Tipikor, Kriptografi, Ciphertext Police Attribute Based Encryption, CP-ABE.*

PENDAHULUAN

Tindak pidana korupsi (tipikor) merupakan suatu perbuatan dengan penyuapan manipulasi dan perbuatan melawan hukum yang merugikan keuangan negara atau perekonomian negara serta merugikan kesejahteraan atau kepentingan rakyat. Tipikor dianggap sebagai perbuatan yang sangat keji dan merugikan masyarakat oleh karena itu tipikor sangat dilarang karena bisa merusak sendi-sendi tatanan kehidupan bermasyarakat berbangsa dan bernegara. Perkembangan tipikor di Indonesia sungguh sangat mengkhawatirkan dan setiap tahun terus mengalami peningkatan seperti yang dirilis oleh Komisi Pemberantasan Korupsi (KPK) di tahun 2018 KPK melakukan penanganan tindak pidana korupsi dengan rincian: penyelidikan 164 perkara, penyidikan 199 perkara, penuntutan 151 perkara, inkracht 106 perkara, dan eksekusi 113 perkara [1]. Memperhatikan data tersebut bahwa tipikor menjadi salah satu permasalahan sangat serius yang harus mendapat perhatian tidak hanya oleh KPK dan penegak hukum lainnya tetapi oleh seluruh lapisan masyarakat Indonesia. Tingkat partisipasi masyarakat menjadi salah satu kunci keberhasilan penanganan tipikor di Indonesia.

Selain KPK lembaga pemerintah yang memiliki tugas dalam menangani tipikor adalah Kejaksaan Tinggi Republik Indonesia. Kejaksaan Tinggi Bali (Kejati Bali) sebagai salah satu lembaga Kejaksaan di Indonesia telah memfasilitasi masyarakat untuk melakukan pengaduan tipikor melalui pos pelayanan hukum dan pengaduan masyarakat yang ada di Kantor Kejati Bali. Selain pos

pelayanan hukum dan pengaduan masyarakat, Kejati Bali juga memfasilitasi masyarakat untuk melakukan pengaduan tipikor melalui halaman website.

Dari observasi awal yang dilakukan bahwa fasilitas pengaduan di halaman website Kejati Bali belum lengkap karena hanya memfasilitasi masyarakat untuk memberikan data pelapor berupa nama, alamat, email dan data pengaduan berupa topik/judul aduan, keterangan aduan serta fasilitas keamanan berupa *captcha* [2]. Pada form pengaduan ini tidak memiliki fitur tentang perlindungan privasi dan kerahasiaan data pengaduan.

Memperhatikan permasalahan tersebut maka pada penelitian ini akan dikembangkan sistem pengaduan online tipikor yang dilengkapi dengan perlindungan data pengaduan dengan cara menerapkan salah satu metode enkripsi yaitu Ciphertext-Police Attribute Based Encryption (CP-ABE). Implementasi CP-ABE ini menempatkan kebijakan akses pada data yang dienkripsi, dan satu set atribut deskriptif berada di kunci pribadi pengguna. Jika atribut yang ditetapkan memenuhi kebijakan akses, pengguna dapat mendeskripsikan data pengaduan.

Dengan skema ini keamanan data pengaduan menjadi terjaga, dimana pada setiap data telah ditempatkan kebijakan akses yang terenkripsi, dan satu set atribut deskriptif berada di kunci pribadi pelapor. Sehingga data pengaduan (Ciphertext) hanya bisa dideskripsikan oleh penerima pengaduan jika himpunan atribut kunci penerima sesuai dengan atribut ciphertext.

TINJAUAN PUSTAKA

Penelitian Terdahulu

Penelitian tentang Peran Serta Masyarakat Dalam Pencegahan Tindak Pidana Korupsi Pengelolaan Keuangan Dana Desa dilakukan oleh [3]. Hasil penelitiannya menunjukkan bahwa pemahaman warga Desa Cau Blayu masih sangat minim tentang tindak pidana korupsi, serta pentingnya peran warga dalam mencegah terjadi tindak pidana korupsi khususnya sehubungan pengelolaan dana desa. Dalam penelitiannya juga menyampaikan bahwa perlu dukungan dan peran serta masyarakat dalam mengawasi dan melaporkan penyalahgunaan dana desa sebagai salah satu upaya pencegahan korupsi untuk meningkatkan efektifitas, pembangunan dan kesejahteraan masyarakat desa di sekitarnya.

Penelitian tentang Kebijakan Hukum Pidana dalam Upaya Meningkatkan Peran Serta Masyarakat dalam Pencegahan dan Pemberantasan Tindak Pidana Korupsi dilakukan oleh [4]. Hasil penelitiannya menunjukkan bahwa hukum pidana di Indonesia telah menganut sistem dimana peran serta masyarakat memiliki ruang untuk turut berperan dalam upaya pencegahan dan pemberantasan tindak pidana korupsi. Hasil penelitiannya juga mengungkapkan bahwa perlu ada peran serta masyarakat dalam pencegahan dan pemberantasan tindak pidana korupsi.

Penelitian tentang pengembangan perangkat lunak menggunakan konsep otentikasi anonim dilakukan oleh [5]. Dalam penelitiannya telah dikembangkan sebuah perangkat lunak untuk penyimpanan data di awan, dimana sistem yang dikembangkan mampu melakukan otentikasi pengguna tanpa mengetahui detail pengguna dari sistem tersebut. Sistem yang dikembangkan juga memfasilitasi pengguna untuk melakukan enkripsi dan deskripsi file dengan ABE dan *Attribute Based Signature* (ABS).

Penelitian tentang perlindungan privasi pengguna *Cloud Base Personal Health Record* (CB-PHR) System dilakukan oleh [6]. Dalam penelitiannya menggunakan ABE sebagai metode enkripsi *public domain*, dan menggunakan metode *Anonymous Multi-Receiver Identity-based Encryption* untuk melakukan enkripsi

personal domain. Hasil penelitiannya menunjukkan sistem CB-PHR yang dikembangkan terbukti aman, memberikan perlindungan privasi, skalabel, dan efisien.

Mempelajari beberapa penelitian yang telah dilakukan sebelumnya yang membahas tentang pencegahan tindak pidana korupsi, kebijakan hukum pidana dalam upaya meningkatkan peran serta masyarakat dalam pencegahan dan pemberantasan tindak pidana korupsi, pengembangan perangkat lunak menggunakan metode otentikasi anonim, dan perlindungan privasi pengguna CB-PHR, belum ada penelitian yang mengimplementasikan CP-ABE pada sistem pengaduan tindak pidana korupsi di Kejaksaan Tinggi Bali. Diharapkan dengan adanya sistem ini keamanan data pengaduan pengaduan tindak pidana korupsi lebih baik. Perlindungan dan kerahasiaan data pengaduan lebih terjaga sehingga masyarakat sebagai pelapor merasa lebih berani mengadukan kejadian tindak pidana korupsi yang terjadi di lingkungannya.

Tindak Pidana Korupsi (Tiikor)

Setiap orang yang dengan tujuan menguntungkan diri sendiri atau orang lain atau suatu korporasi, menyalahgunakan kewenangan kesempatan atau sarana yang ada padanya karena jabatan atau kedudukan yang dapat merugikan keuangan negara atau perekonomian negara bisa disebut korupsi. Suatu perbuatan dikatakan korupsi menurut hukum positif Indonesia, jika telah memenuhi empat unsur sebagai berikut [7]:

1. Melawan hukum, pengertian yang dimaksud adalah mencakup perbuatan melawan hukum baik secara formal maupun materiil. Melawan hukum secara formal berarti suatu perbuatan tersebut dilakukan dengan melanggar peraturan atau perundang-undangan, namun tetap dapat dikatakan melawan hukum apabila perbuatan tersebut dianggap tercela karena tidak sesuai dengan rasa keadilan masyarakat maupun norma-norma kehidupan sosial yang tumbuh dan berkembang dimasyarakat.
2. Memperkaya diri sendiri, orang lain, atau korporasi. Suatu perbuatan dikatakan korupsi jika perbuatan tersebut menyebabkan bertambahnya kekayaan bagi pelaku perbuatan tersebut, orang lain (yang diuntungkan

- bukan pelaku langsung) atau suatu lembaga (korporasi).
3. Dapat merugikan keuangan negara atau perekonomian negara. Keuangan negara yang dimaksud adalah seluruh kekayaan negara dalam bentuk apapun, yang dipisahkan atau yang tidak dipisahkan. Termasuk didalamnya segala bagian kekayaan negara dan segala hak dan kewajiban yang timbul karena:
 - a. Berada dalam penguasaan, pengurusan dan pertanggungjawaban pejabat lembaga negara baik di tingkat pusat maupun daerah.
 - b. Berada dalam penguasaan, pengurusan dan pertanggungjawaban Badan Usaha Milik Negara (BUMN) atau Badan Usaha Milik Daerah (BUMD), yayasan, badan hukum dan perusahaan yang menyertakan modal pihak ketiga berdasarkan perjanjian dengan negara. (Penjelasan Undang-Undang Nomor 31 Tahun 1999 tentang Tindak Pidana Korupsi).
 4. Menyalahgunakan kewenangan, kesempatan atau sarana karena jabatan atau kedudukan yang melekat pada jabatan tersebut, artinya suatu perbuatan dikatakan korupsi jika perbuatan tersebut dilakukan dengan menyalahgunakan kedudukan atau jabatan yang dipercayakan negara pada seseorang. Kewenangan yang dimaksud bukan hanya terdapat pada diri penyelenggara negara, tetapi juga kewenangan yang diberikan oleh pemerintah kepada pribadi, pihak swasta, lembaga swadaya masyarakat, atau lembaga lainnya yang berkaitan dengan masalah keuangan atau perekonomian negara.

Peran Serta Masyarakat dalam Pemberantasan Tipikor

Dalam Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2000 Tentang Tatacara Pelaksanaan Peran Serta Masyarakat dan Pemberian Penghargaan dalam Pencegahan dan Pemberantasan Tindak Pidana Korupsi, diatur dan disebutkan dalam Bab III peraturan tersebut, yang secara rinci dapat dijabarkan, sebagai berikut [8]:

1. Pasal 7 ayat (1): setiap orang, organisasi masyarakat atau lembaga swadaya masyarakat yang telah berjasa dalam usaha membantu upaya pencegahan atau pemberantasan tindak pidana

korupsiberhak mendapat penghargaan. Ayat (2) menyebutkan: penghargaan sebagaimana dimaksud dalam ayat (1) dapat berupa piagam atau premi.

2. Pasal 8: ketentuan mengenai tata cara pemberian penghargaan serta bentuk dan jenis piagam sebagaimana dimaksud dalam pasal 7 ayat (2) ditetapkan dengan keputusan Menteri hukum dan Perundang-undangan.
3. Pasal 9: besar premi sebagaimana dimaksud dalam pasal 7 ayat (2) ditetapkan paling banyak sebesar 2% (dua persen) dari nilai kerugian keuangan Negara yang dikembalikan.
4. Pasal 10 ayat (1): piagam diberikan kepada pelapor setelah perkara dilimpahkan ke Pengadilan Negeri. Ayat (2): penyerahan piagam sebagaimana dimaksud dalam ayat (1) dilakukan oleh penegak hukum atau Komisi.

Pasal 11 ayat (1): premi diberikan kepada pelapor setelah putusan pengadilan yang memidanakan terdakwa memperoleh kekuatan hukum tetap. Ayat (2): penyerahan premi sebagaimana dimaksud dalam ayat (1) dilakukan oleh Jaksa Agung atau pejabat yang ditunjuk.

Ciphertext Police - Attribute Based Encryption (CP-ABE)

Attribute Based Encryption (ABE) termasuk ke dalam jenis enkripsi asimetric. Metode ini diperkenalkan oleh Sahai dan Waters [1] di 2005. ABE termasuk ke dalam jenis *public key encryption* dimana kunci rahasia dari pengguna dan ciphertext tergantung pada atribut pengguna seperti tempat lahir, jabatan di organisasi dan atribut lainnya. Ciphertext hanya bisa didekripsikan jika himpunan atribut kunci pengguna sesuai dengan atribut ciphertext. Dilihat dari kebijakan akses ABE diklasifikasikan menjadi dua skema [2] yaitu Key-Policy Attribute Based Encryption (KP-ABE) dan Ciphertext-Policy Attribute Based Encryption (CP-ABE). Pada skema KP-ABE kebijakan akses ditempatkan ke kunci pribadi pengguna, dan sekumpulan atribut deskriptif ada di data terenkripsi. Jika satu set atribut memenuhi kebijakan akses, pengguna dapat mendekripsikan pesan. Jika tidak, pengguna tidak bisa mendekripsikan pesan tersebut. Sedangkan pada CP-ABE kebijakan akses ditempatkan pada data yang dienkripsi, dan satu set atribut deskriptif

berada di kunci pribadi pengguna. Jika atribut yang ditetapkan memenuhi kebijakan akses, pengguna dapat mendeskripsikan data pengguna.

METODE PENELITIAN

Tahapan Penelitian

Beberapa tahapan dilakukan dalam melakukan penelitian ini mulai dari melakukan observasi, studi literature, melakukan analisis kebutuhan, membuat desain sistem, mengimplementasikan sistem dan melakukan evaluasi berupa pengujian fungsional dari sistem yang telah dikembangkan. Berikut Gambar 1 merupakan tahapan penelitian yang dilakukan.



Gambar 1 Tahapan Penelitian

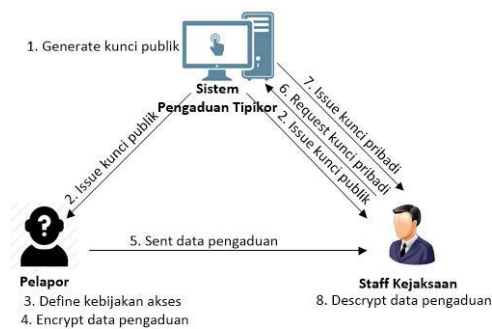
Gambar 1 menunjukkan bahwa tahapan penelitian dimulai dengan melakukan observasi proses pengaduan tipor di Kejaksaan Tinggi Bali, serta mempelajari beberapa penelitian sebelumnya yang terkait dengan pengaduan tipikor dan implementasi CP-ABE. Berdasarkan hasil observasi dan studi literatur yang dilakukan ditemukan kelemahan pada sistem pengaduan tipikor saat ini seperti yang sudah dipaparkan pada latar belakang masalah penelitian ini.

Dari latar belakang masalah tersebut selanjutnya ditetapkan kebutuhan-fungsional dari sistem pengaduan yang mau dikembangkan. Berdasarkan kebutuhan fungsional yang ditetapkan selanjutnya dibuat desain sistem dan dilanjutkan dengan implementasi atau pengembangan sistem pengaduan tipikor. Hasil pengembangan ini kemudian diuji

sesuai dengan fungsional sistem yang telah ditetapkan sebelumnya menggunakan beberapa skenario uji. Dari hasil pengujian ini akan diambil kesimpulan dari pengembangan sistem pengaduan tipikor dengan skema CP-ABE.

Skema CP-ABE untuk Pengaduan Tipikor

Pada bagian ini akan dijelaskan bagaimana arsitektur implementasi CP-ABE untuk pengaduan tipikor, detail dari proses pengaduan dapat dilihat pada Gambar 2 berikut ini.



Gambar 2. Skema CP-ABE untuk Pengaduan Tipikor

Gambar 2 memperlihatkan proses pengaduan tipikor mulai dari pembuatan kunci public oleh sistem pengaduan tipikor, pendistribusian kunci publik kepada pelapor dan staff kejaksanaan. Selanjutnya proses mendefinisikan kebijakan-kebijakan akses oleh pelapor. Pelapor akan mendefinisikan sekumpulan atribut deskriptif dan nilai ambang batas untuk setiap data yang dimiliki. Setelah kebijakan akses didefinisikan, selanjutnya pelapor bisa melakukan enkripsi data pengaduan dan seluruh kebijakan akses akan melekat pada data yang terenkripsi. Misalkan pemilik data membuat kebijakan akses berupa sekumpulan atribut deskriptif {Pegawai, PNS, Programmer} dengan nilai ambang batas {2}. Jika penerima pesan ingin mendeksiprikan pesan yang terenkripsi, jumlah atribut kunci pribadi penerima perlu dua atau lebih dari dua atribut dalam pesan yang terenkripsi, sehingga penerima pesan harus memiliki atribut { Pegawai, PNS} untuk mendeksiprikan dan membaca pesan. Data yang sudah dienkripsi bisa dikirim sehingga bisa diterima di akun staff kejaksanaan tinggi.

Untuk membuka isi data pengaduan yang diterima, staff kejaksanaan bisa melakukan permintaan kunci ke sistem

pengaduan tipikor dengan memasukan sejumlah atribut yang bersesuaian dengan kebijakan akses pada data pengaduan yang diterima. Sistem pengaduan tipikor akan memberikan respon permintaan kunci, dimana kunci akan diberikan apabila atribut yang dimasukan memiliki kecocokan dengan kebijakan akses yang ada pada data pengaduan. Apabila kunci sudah diterima, staff kejaksaaan bisa mendeskripsikan data pengaduan menjadi plaintext sehingga isi pengaduan bisa dibaca.

HASIL DAN PEMBAHASAN

Form Registrasi Pengguna

Sebelum pengguna menggunakan sistem pengaduan tipikor ini, pengguna harus melakukan pendaftaran dengan mengisi form *registrasi* seperti yang ditunjukkan pada Gambar 3 berikut ini.

Gambar 3 Form Registrasi Pengguna

Setelah melakukan pendaftaran di form registrasi pengguna, pengguna bisa menggunakan sistem dengan melakukan login terlebih dahulu seperti yang terlihat pada Gambar 4 berikut ini.

Gambar 4. Form Login Pengguna
Form Enkripsi, Pengaduan dan Pengaduan Masuk

Form ini digunakan oleh pelapor untuk membuat pengaduan kejadian tipikor. Sebelum melaporkan kejadian tipikor, data pengaduan bisa dienkripsi terlebih dahulu menggunakan form enkripsi seperti yang terlihat pada Gambar 5 berikut ini.

Gambar 5. Form Enkripsi dan Pengaduan

Pada Gambar 5 terlihat untuk melakukan enkripsi data pengaduan, pelapor harus menambahkan sejumlah atribut yang menjadi kebijakan akses yang melakat pada data pengaduan yang terenkripsi. Dan setelah file dienkripsi pelapor bisa mengirim pengaduan tersebut dengan menekan tombol "Send". Apabila data pengaduan terkirim, Staff Kejaksaan Tinggi akan menerima data pengaduan masuk di menu "File Aduan" seperti yang ditunjukkan pada Gambar 6 berikut ini.

Gambar 6. Pengaduan Masuk

Form Permintaan Kunci dan Deskripsi Data Pengaduan

Untuk melihat pengaduan yang masuk pada Gambar 6, Staff Kejaksaan Tinggi harus melakukan permintaan kunci menggunakan form permintaan kunci seperti yang ditunjukkan pada Gambar 7 berikut ini.

Gambar 7. Permintaan Kunci

Seperti yang terlihat pada Gambar 7 untuk mendapatkan kunci Staff Kejaksaan Tinggi harus memasukan sejumlah atribut yang bersesuaian dengan kebijakan akses pada file tersebut, dan apabila atribut yang dimasukan tidak sesuai maka akses permintaan kunci akan ditolak. Apabila set atribut yang dimasukan sesuai, maka Staff Kejaksaan Tinggi akan diberikan kunci sehingga bisa digunakan untuk mendeskripsikan data pengaduan seperti yang terlihat pada Gambar 8 berikut ini.

Gambar 8 . Form Deskripsi File

PENGUJIAN SISTEM

Proses pendaftaran pengguna, enkripsi data pengaduan, pengiriman data pengaduan, permintaan kunci, hingga proses deskripsi sudah dilakukan pengujian berdasarkan skenario yang telah dibuat sebelumnya. Detail hasil pengujian dapat dilihat pada Tabel 1 berikut ini :

Tabel 1: Hasil Pengujian

No.	Fungsional	Skenario	Hasil	Ket
1	Pendaftaran Pengguna	Pengguna mengakses halaman register, melengkapi form registrasi pengguna, dan menekan tombol "Register"	Pendaftaran berhasil dan berada di halaman form login pengguna	sesuai
2	Login Pengguna	Pengguna memasukan username dan password pada form login dan menekan tombol "Login"	Login berhasil dan berada di halaman pengaduan apabila login sebagai pelapor, atau berada di halaman file aduan apabila login sebagai staf kejaksaan tinggi	sesuai
3	Enkripsi Data Pengaduan	Pengguna melengkapi data pengaduan di form pengaduan, memilih beberapa atribut sebagai kebijakan akses dan menekan tombol "Encrypt".	Proses enkripsi berhasil, data pengaduan yang sebelumnya berupa plaintext menjadi ciphertext	sesuai
4	Kirim Pengaduan	Pengguna masih berada di form pengaduan, dan data pengaduan sudah dalam bentuk enkripsi, kirim pengaduan dengan menekan tombol "Send"	Data pengaduan terkirim dari pelapor dan masuk ke dalam file aduan pada akun staff kejaksaan tinggi	sesuai
6	Daftar Pengaduan Masuk	Login staf kejaksaan tinggi berhasil dan memilih menu file aduan	Sistem bisa menampilkan file pengaduan yang masuk dan dilengkapi buton link untuk melihat isi pengaduan.	sesuai
7	Permintaan Kunci	Staff kejaksaan tinggi melengkapi beberapa atribut pada Form Permintaan Kunci dan menekan tombol Request	Sistem akan memberikan kunci apabila atribut yang dimasukan sesuai kebijakan akses yang ditetapkan oleh pelapor saat melakukan enkripsi data aduan, dan sistem akan memberikan respon penolakan apabila atribut yang dimasukan tidak memiliki kecocokan dengan kebijakan akses	sesuai
8	Deskrip Data Pengaduan	Staff kejaksaan tinggi berada pada form deskripsi pengaduan, memasukan kunci yang sudah diterima sebelumnya, dan menekan tombol "Decrypt"	Sistem memberikan respon deskripsi berhasil, dan menampilkan data pengaduan dalam bentuk plaintext	sesuai

SIMPULAN

Implementasi skema Ciphertext-Police Attribute Based Encryption untuk pengaduan tindak pidana korupsi, apat melakukan enkripsi dengan sejumlah atribut sebagai kebijakan akses, menghasilkan kunci, mengirim pengaduan, mendeskripsikan data pengaduan menggunakan kunci. Hasil evaluasi menunjukkan sistem dapat berjalan dengan baik sesuai dengan skenario pengujian yang ditetapkan.

DAFTAR PUSTAKA

- [1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," *Lect. Notes Comput. Sci.*, vol. 3494, pp. 457–473, 2005.
- [2] Rekapitulasi Tindak Pidana Korupsi Komisi Pemberantasan Korupsi. Diakses dari <https://acch.kpk.go.id/id/statistik/tindak-pidana-korupsi>. (4 November 2019).
- [3] Form Pengaduan Masyarakat Kejaksaan Tinggi Bali. Diakses dari <https://kejatibali.go.id/index.php/pengaduan>. (4 November 2019).
- [4] Putra I. M. W, Widhiyaatuti I. G. A. A. D, Putra I. P. R. A. 2018. Octa Comitas 1 : 1 – 16. Peran Serta Masyarakat Dalam Pencegahan Tindak Pidana Korupsi Pengelolaan Keuangan Dana Desa, Studi Di Desa Cau Belayu, Kecamatan Marga, Kabupaten Tabanan, Propinsi Bali.
- [5] Naibaho P. Y. H, Purwoto, Pujiyono. 2016. Diponegoro Low Journal. Volove 5. Nomor 4. Kebijakan Hukum Pidana Dalam Upaya Meningkatkan Peran Serta Masyarakat Dalam Pencegahan⁽¹⁾ Dan Pemberantasan Tindak Pidana Korupsi.
- [6] Linawati, Suryawan I. G. T. Sudarma M. 2017. IJSIA. Vol. 11. No. 1. Anonymous Authentication with Centralize Access Control of Data Storage in Cloud.
- [7] Wang C, Xu X, Shi D, Fang J. 2015. Informatica 39 375-382. Privacy-preserving Cloud-based Personal Health Record System Using Attribute-based Encryption and Anonymous Multi-Receiver Identity-based Encryption.
- [8] Putra M. G. A, Dahlan, Mahfud. 2018. Syah Kuala Low Journal. Vol. 2 (2). Kendala Yang Dihadapi Oleh Kejaksaan Tinggi Aceh Dalam Pemberantasan Tindak Pidana Korupsi.
- [9] Ridwan. 2014. Kanun Jurnal Ilmu Hukum. No. 16. Th. XVI. pp. 385-399. Upaya Pencegahan Tindak Pidana Korupsi Melalui Peran Serta Masyarakat.
- [10] Ruj S, Stojemenovic M, Nayak A. 2014. Ieee Transactions On Parallel And Distributed Systems. Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds
- [11] Suryawan I. G. T, Linawati, Handika I. P. S. IEE Explore Digital Library Ciphertext-Police Attribute Based Encryption Performance on Notebook Device