Analisa Keamanan Dan Privasi Data Pada Sistem Penyimpanan Icloud

Daffa Ebtra Satria[1*], Fajar Wahyu Hanafi[2], Marcelino Jonatan San Putra[3], Yosua Arematheа Novantoro[4]

[1]*Teknik Informatika*
Universitas Duta Bangsa Surakarta
[1*]220103052@mhs.udb.ac.id

[2] *Teknik Informatika*
Universitas Duta Bangsa Surakrta
[2]220103057@mhs.udb.ac.id

[3]*Teknik Informatika*
Universitas Duta Bangsa Surakrta
[3]220103063@mhs.udb.ac.id

[4]*Teknik Informatika*
Universitas Duta Bangsa Surakrta
[4]220103080@mhs.udb.ac.id

Abstrak— **Pada era digital saat ini, isu mengenai privasi dan keamanan data menjadi sangat penting seiring dengan meningkatnya penggunaan layanan penyimpanan awan. Salah satu layanan penyimpnan awan yang populer adalah iCloud dari Apple, yang menawarkan kemudahan penyimpanan dan sinkronasi data antar perangkat. Namun, layanan ini juga menghadirkan tantangan dalam hal keamanan dan privasi data. Penelitian ini bertujuan untuk menganalisis aspek keamanan dan privasi data pada layanan iCloud. Metodelogi yang digunakan adalah literature review dengan mengumpulkan dan menganalisis berbagai sumber ilmiah yang relevan. Hasil penelitian menunjukkan bahwa Apple telah menerapkan berbagai mekanisme keamanan untuk melindungi data pengguna, seperti autentikasi dua faktor, penggunaan enkripsi data end-to-end dan AES. Namun, pengguna harus tetap waspada terhadap ancaman seperti pencurian data dan serangan siber lainnya.Diharapkan penelitian ini memberikan pemahaman yang lebih baik tentang bagaimana cara Apple melindungi data pengguna dan bagaimana meningkatkan keamanan dan privasi data pada layanan iCloud.**

Kata kunci— iCloud, penyimpanan awan, keamanan data, privasi data.

Abstract— **In the contemporary digital age, concerns pertaining to data privacy and security have assumed heightened significance, concomitant with the proliferation of cloud storage services. One of the most widely used cloud storage services is Apple's iCloud, which provides a convenient platform for storing and synchronizing data across multiple devices. Nevertheless, this service also presents challenges in terms of data security and privacy. This research project aims to analyze the security and data privacy aspects of the iCloud service. The methodology employed was a literature review, whereby various relevant scientific sources were collected and analyzed. The results demonstrate that Apple has implemented a range of security mechanisms to safeguard user data, including two-factor authentication, end-to-end data encryption, and AES. However, users must remain vigilant against potential threats such as data theft and other cyber attacks. It is hoped that this research will facilitate a deeper understanding of Apple's data protection measures and inform improvements to data security and privacy on the iCloud service.**

Keywords— iCloud, cloud storage., data security, data privacy.

I. PENDAHULUAN

Di era globalisasi yang semakin pesat, teknologi informasi telah menjadi salah satu pilar utama yang menunjang perkembangan diberbagai bidang kehidupan. Selain itu, di jaman yang serba modern sekarang ini banyak kegiatan maupun aktivitas baik di lingkup sekolah, Masyarakat, ataupun lainnya yang perlu didokumentasikan, disimpan, dan dapat diakses dimana saja ketika dibutuhkan[1]. Salah satu inovasi teknologi terkait permasalahan tersebut yaitu dengan munculnya Cloud Computing sebagai solusi untuk memecahkan masalah ini. Cloud Computing merupakan sebuah teknologi yang memungkinkan penggunaan alat seperti smartphone, laptop, ataupun komputer melalui internet untuk menyimpan data dan informasi. Dengan Cloud Computing, pengguna dapat menyimpan dan mengakses data informasi yang tersimpan didalam cloud dari mana saja dan kapan saja, tanpa perlu khawatir jika lupa membawa flashdisk atau hardisk karena layanan ini dapat diakses hanya dengan menggunakan internet dan pengguna hanya perlu membuka aplikasi atau website layanan cloud seperti Google Drive, Dropbox, iCloud, dan lain sebagai nya [2].

iCloud merupakan salah satu layanan penyimpanan cloud yang dikembangkan oleh apple dan dirancang untuk integrasi dengan perangkat Apple seperti iPhone, iPad, dan Mac. Layanan cloud yang dikembangkan Apple ini memberikan kapasitas penyimpanan yang dapat diperluas dan disinkronisasi datanya secara otomatis antar perangkat. Selain itu, Icloud menawarkan kemudahan dan efisiensi bagi pengguna dalam mengelola data mereka seperti foto, dokumen, hingga aplikasi. Namun, dengan kemudahan yang ditawarkan oleh iCloud, muncul pula tantangan signifikan terkait keamanan dan privasi data. Pengguna perlu memahami potensi risiko seperti pencurian data, kebocoran informasi pribadi, serta serangan siber yang dapat merusak integritas data yang disimpan pada layanan ini.

Pada penelitian sebelumnya, Arif et al. (2019) telah melakukan penelitian yang membandingkan dua layanan cloud storage terkenal yaitu, Google Cloud dan iCloud. Dalam penelitian ini membahas tentang sejarah berdirinya hingga perkembangan setiap layanan, dan juga fitur-fitur unggulan yang disediakan oleh keduanya. Hasil dari penelitian menunjukkan bahwa kedua layanan tersebut memiliki kesamaan kelebihan, seperti dalam hal skalabilitas, replikasi, dan kemudahan akses di berbagai lokasi. Dengan kesamaan keunggulan tersebut terdapat perbedaan yang cukup besar dari kedua layanan ini, seperti dalam hal keamanan sistem, dan juga ekosistem layanan yang menjadi pertimbangan uitama penggunan dalam memilih platform yang tepat [3]. Sedangkan pada penelitian yang dilakukan oleh O'rinov dkk pada tahun 2021 membahas mengenai gambaran umum sistem deteksi anomali pada cloud seperti jenis, metode dan masalah yang dihadapi pada setiap metode yang mengakibatkan ketidak efisien dalam pendeteksiannya. Dalam penelitian tersebut O'rinov dkk membandingkan langkah-langkah keamanan dari penyedia layanan cloud seperti Dropbox, Google Drive, dan iCloud yang ditemukan bahwa hampir setiap penyedia layanan memiliki langkah keamanan yang mirip serta memiliki kelebihan dan kekurangannya masing-masing [4].

Berdasarkan uraian diatas, penelitian ini bertujuan untuk menganalisis aspek privasi dan keamanan data pada sistem penyimpanan berbasis cloud yang digunakan oleh Apple. Penelitian ini akan mengkaji berbagai mekanisme keamanan yang diterapkan, mengidentifikasi potensi risiko, dan mengevaluasi langkah mitigasi yang diambil Apple untuk melindungi data pengguna. Oleh karena itu, penelitian ini diharapkan dapat memberikan pemahaman mengenai perlindungan data pada layanan cloud Apple dan memberikan rekomendasi untuk meningkatkan keamanan data dan privasi data pengguna.

II. METODOLOGI PENELITIAN

Pada penelitian ini, dalam analisa yang dilakukan menggunakan metode literatur review. Literature review merupakan serangkaian kegiatan untuk mengumpulkan data pustaka dan informasi terkait objek penelitian melalui sumber-sumber seperti jurnal atau artikel, buku, serta sumber-sumber lainnya yang dapat digunakan untuk dijadikan landasan dalam pembahasan atau isi [5]. Adapun tahapan-tahapan yang dilakukan dalam penelitian ini diantaranya yaitu:

1. Menentukan ruang lingkup topik yang akan direview, dalam penelitian ini ruang lingkup topiknya adalah keamanan dan privasi data pada penyimpanan cloud khususnya iCloud Apple.
2. Mengumpulkan literatur, pada penelitian ini pengumpulan dilakukan dengan mencari penelitian yang masih berkaitan dengan penyimpanan cloud.
3. Mengidentifikasi sumber literatur, pada penelitian ini identifikasi dilakukan dengan cara memilah sumber rujukan yang didapatkan.
4. Menulis tinjauan literatur, tahap terakhir pada penelitian ini adalah mengambil substansi pada sumber yang didapat dan kemudian dievaluasi serta dituliskan kembali.

Adapun temuan literatur review terkait diantaranya yaitu :

Pada penelitian yang telah dilakukan oleh Z. Masyhur, A. Rizaldy, P. Kartini (2021) telah melakukan penelitian mengenai Studi Literatur dan memberikan sebuah hasil Keamanan dan Privasi Data Sistem Cloud Computing Pada Platform Google Drive. dengan Membandingkan keamanan dan privasi data pada Google Drive memiliki kelebihan Menyediakan analisis komparatif akan tetapi tidak membahas secara mendalam enkripsi end-to-end [1].

Pada penelitian yang telah dilakukan oleh Agus Irawan, Destiawati Fitriana, Dhika Harry (2019), telah melakukan sebuah penelitian dengan judul Perbandingan Cloud Computing Micosoft Onedrive Dropbox dan Google Drive. dengan metode studi literatur Membandingkan layanan cloud terkenal yang menghasilkan bahwa OneDrive, Dropbox, dan Google Drive memiliki keunggulan dan kelemahan masing-masing. Pembahasan pada studi memberikan analisis mendalam pada berbagai layanan namun tidak berfokus pada layanan iCloud [2].

Pada penelitian yang telah dilakukan oleh O. Toxirjonovich, A. Zaylobiddinovich, A. Vohidjon O'g'li (2022), yang telah melakukan sebuah penelitian tantang An Overview Of Anomaly Detection Systems In Cloud Networks And An Overview Of Security Measures In Cloud Storage. Dengan tujuan untuk meninjau sistem deteksi anomali pada jaringan cloud dengan metode studi literatur dan memberikan hasil bahwa banyak penyedia layanan cloud memiliki langkah keamanan yang mirip. Studi ini memiliki kelebihan dengan menyediakan analisis komparatif dan memiliki kekurangan yaitu kurang nya fokus pada serangan siber spesifik pada iCloud [4].

Pada penelitian yang telah dilakukan oleh Hera Arif , Hassan Hajjdiab, Fatima Al Harbi , Mohammed Ghazal (2019), telah melakukan sebuah penelitian mengenai Comparison between Google Cloud Service and iCloud. Dengan tujuan Membandingkan fitur dan performa Google Cloud Platform dan iCloud. Pada penelitian tersebut menggunakan metode studi literatur yang menghasilkan bahwa Google Cloud Platform memiliki fitur yang lebih baik dan berkinerja lebih baik di pasar dibandingkan iCloud. Perbandingan yang mendalam tentang fitur layanan iCloud menjadi kelebihan pada studi ini, sedangkan pada studi ini meliliki kekurangan pada tidak adanya analisis mendalam tentang biaya, keamanan, dan kemudahan penggunaa [3]..

III. HASIL DAN PEMBAHASAN

A. ICloud

iCloud adalah layanan cloud dari Apple yang diluncurkan pada tahun 2011. iCloud menawarkan penyimpanan data yang mencakup foto, video, musik, dokumen, dan data terkait aplikasi yang dimana data yang tersimpan didalamnya dapat diakses dari mana saja melalui internet. Layanan pada iCloud memiliki rentang harga penawaran yang bervariasi mulai dari penyimpanan secara gratis sebesar 5 GB, serta terdapat opsi penambahan penawaran penyimpanan 50 GB dengan harga Rp. 15.000, 200 GB dengan harga Rp. 45.000, 2 TB dengan harga Rp. 149.000, 6TB senilai Rp. 449.000, dan 12 TB senila i Rp. 899.000 [3]. Selain itu, layanan iCloud memiliki kelebihan yang diantaranya seperti integritas data yang baik pada produk dalam ekosistem mereka, sinkronisasi otomatis pada perangkat yang terhubung pada akun iCloud tersebut, pencadangan data secara otomatis yang dapat memudahkan pemulihan data apabila terjadi kehilangan atau kerusakan perangkat, dan menjamin privasi dan keamanan data pengguna. Namun, iCloud juga memiliki beberapa kekurangan yang diantaranya seperti biaya penambahan penyimpanan yang cukup tinggi, keterbatasan fungsionalitas pada produk non-Apple, dan ketergantungan terhadap konektivitas internet yang stabil karena dibutuhkan dalam sinkronisasi data antar perangkat maupun pencadangan data secara otomatis.

B. Mekanisme Keamanan dan Privasi Data

ICloud, sebagai layanan penyimpanan awan dari Apple, memberikan prioritas tinggi pada keamanan dan privasi data pengguna dengan menerapkan berbagai metode keamanan yang canggih dan kebijakan yang ketat. Salah satu pondasi dari mekanisme keamanan ini adalah perlindungan Apple ID, yang dimana setiap Apple ID baru diwajibkan menggunakan autentikasi dua faktor yang berguna untuk melindungi pengguna dari upaya penipuan yang mencoba mengakses akun mereka. Selain autentikasi dua faktor, iCloud juga menerapkan berbagai macam enkripsi data yang dimana kunci enkripsi tersebut disimpan di pusat data Apple sehingga hal tersebut dapat membantu perusahaan dalam membantu pengguna untuk melakukan pemulihan data jika diperlukan [6]. Selain itu, Apple iCloud juga mendukung enkripsi end-to-end untuk melindungi data sensitif yang disimpan didalam iCloud [7]. Berikut ini akan dibahas beberapa mekanisme keamanan pada iCloud diantaranya yaitu.:

1) Apple ID

Apple ID merupakan akun penting yang digunakan untuk mengakses layanan Apple. Selain itu, penting bagi pengguna untuk menjaga keamanan Apple ID tersebut untuk mencegah dari akses yang tidak sah. Oleh karena itu, terkait hal tesebut Apple menyarankan atau menganjurkan pembuatan kata sandi yang kuat dengan perbaduan antara huruf dan angka serta minimal delapan karakter, Apple juga menyarankan agar kata sandi yang dibuat tidak

mengandung tiga atau lebih karakter yang identik berurutan dan bukan kata sandi umum. Apple juga memberi tahu pengguna melalui sebuah email ataupun notifikasi jika terdapat perubahan penting dalam akun, seperti perubahan kata sandi atau jika Apple ID digunakan untuk masuk ke perangkat baru. Selain hal tersebut, Apple juga menerapkan berbagai macam kebijakan kamanan, termasuk pembatasan percobaan masuk dan pengaturan ulang kata sandi, pengawasan penipuan aktif, serta peninjauan berkala untuk memastikan keamanan pengguna tetap terjaga[8].

2) Autentikasi Dua Faktor

Autentikasi dua faktor atau 2FA merupakan sebuah lapisan tambahan yang dimiliki oleh suatu akun selain kata sandi yang harus dimiliki sebelum mengakses akun yang dimiliki [9]. Pengguna yang mengaktifkan fitur 2FA dalam akun mereka biasanya harus memasukkan nama pengguna dan kata sandi sebagai langkah pertama. Setelah informasi akun yang dimasukkan ini diversifikasi, sistem akan meminta pengguna untuk memberikan faktor kedua, yaitu kode sandi sekali pakai (OTP) yang diterima melalui sebuah SMS ataupun pesan pada Email mereka. Dengan memasukkan kode OTP tersebut, pengguna dapat menunjukkan kepemilikkan perangkat yang terdaftar untuk mengkonfirmasi identitas mereka sehingga hal ini dapat menghindari dari upaya penipuan yang mencoba mengakses akun mereka [10]. Dalam konteks penelitian ini, penggunaan 2FA pada iCloud sangat penting untuk menjaga keamanan dan privasi data sensitif yang disimpan didalamnya seperti foto, dokumen, atau informasi pribadi lainnya. Selain itu kode OTP 2FA pada iCloud tidak hanya dikirimkan melalui SMS atau email, tetapi juga dapat menggunakan aplikasi autentikasi yang lebih aman seperti Google Authenticator atau Apple's own built-in authenticator, sehingga hal tersebut menambah perlindungan terhadap serangan phising.

3) Enkripsi Data

Dalam pengamanan enkripsid data, iCloud menerapkan beberapa metode seperti enkripsi data saat dikirm dengan internet menggunakan TLS/SSL, enkripsi data-data yang terismpan di iCloud menggunakan AES, dan enkripsi lanjutan untuk menjamin pengamanan data dengan end-to-end [6][4].

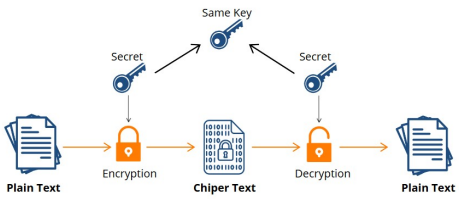
a) Enkripsi saat berjalan menggunakan protokol TLS/SSL

TLS/SSL (Transport Layer Security, Secure Sockets Layer) adalah lapisan keamanan yang melakukan intersepsi dan dekripsi data dalam jaringan untuk melindungi dari serangan konten berbahaya. Perpindahan data merupakan salah satu masalah kritis dalam keamanan siber, oleh karena itu TLS/SSL adalah salah satu alat yang menyediakan saluran komunikasi pribadi antar jaringan. TLS/SSL menyediakan protokol standar untuk mengamankan koneksi dan menjaga keamanan data yang diklasifikasikan. Namun, terkadang peretas menggunakan TLS/SSL untuk membajak informasi dengan menggunakan protokol TLS/SSL yang dimodifikasi selama transfer informasi [11]. Dalam konteks penelitian ini, penggunaan TLS/SSL pada layanan iCloud menunjukan betapa pentingnya protokol keamanan yang kuat untuk menjaga data pengguna. Pada layanan penyimpanan seperti iCloud, yang dimana data milik pengguna disimpan dan diakses melalui internet, penerapan TLS/SSL menjadi sangat penting untuk menjamin data yang dikirimkan antar perangkat pengguna dan server iCloud tetap aman.

b) Enkripsi AES

AES atau yang dikenal sebagai standar enkripsi kunci simetris, merupakan sebuah algoritma yang dikembangkan oleh dua kriptografer asal Belgia yaitu, Joan Daeman dan Vincent Rijmen.

AES memiliki tiga pilihan kunci yang panjangnya berbeda tiap tipenya, diantaranya yaitu tipe AES-128, AES-192, dan AES-256. Dalam proses mengenkripsi dan mendekripsi data AES menggunakan kunci yang sama. Selain itu, sat ini AES merupakan algorimta pengamanan data yang terbaik, karena memliki keamanan yang tinggi serta kecepatan enkripsi dan dekripsi yang efisien[12]. Pada gambar 1, dijelaskan menganai cara kerja AES yang melibatkan pengubahan teks asli (plaintext) menjadi sebuah teks terenkripsi yang tidak dapat dimengerti (chipertext) dengan cara membagi menjadi blok-blok kecil dan dienkripsi setiap bloknya secara terpisah melalui serangkaian langkah, seperti penggantian byte, pergeseran baris, pencampuran kolom, dan penambahan kunci pada tiap putaran sehingga membuat data tersebut sulit untuk dipahami. Selain itu, untuk melihat atau mengembalikan data ke dalam bentuk aslinya diperlukan sebuah kunci yang sama dalam proses deskripsinya [13].



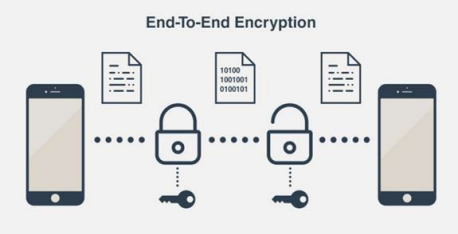
Gambar 1. Enkripsi AES[12]

Dalam konteks penelitian ini, enkripsi AES pada iCloud digunakan untuk melindungi data pengguna yang tersimpan di server. Data yang disimpan di iCloud akan dienkripsi terlebih dahulu sebelum dikirim dan disimpan di server Apple. Contohnya seperti penggunaan AES-128 yang digunakan untuk mengenkripsi data yang tersimpan di server dan AES-256 yang digunakan oleh keychain dengan cara mengenkripsi kata sandi, informasi kartu kredit ataupun data sensitif lainnya yang ada di dalam keychain tersebut [4]. Hal ini menunjukkan bahwa ketika seseorang berhasil mengakses server iCloud, mereka tidak akan dapat memahami data tersebut tanpa kunci enkripsi yang tepat. Selain itu, dalam pengiriman data ke server, proses pengiriman tersebut akan dilindungi oleh protokol TLS/SSL yang memastikan bahwa data tersebut tidak dapat diakses oleh pihak yang tidak sah selama transmisi.

c) Enkripsi End-to-End

Enkripsi ujung ke ujung (End-to-end Encryption) adalah salah satu metode yang paling banyak digunakan untuk mengamankan transmisi informasi melalui Internet. Pada dasarnya enkripsi end-to-end adalah jenis enkripsi dalam sistem komunikasi yang dilakukan terhadap suatu pesan oleh pengirim sebelum dikirim dan didekripsi kembali ketika pesan tersebut sampai ke penerima, dalam artian enkripsi data dilakukan pada sumber pengiriman pesan dan kemudian didekripsi hanya pada tujuan akhir atau penerima pesan. Dengan enkripsi end-to-end, informasi dapat dikirim melalui jaringan menggunakan jalur yang hanya dapat diakses oleh pengirim dan penerima, sehingga informasi yang dikirim oleh pengirim pesan dilindungi oleh kunci khusus yang hanya bisa dideskripsikan oleh penerima [14].

Pada aplikasi chatting modern sering menggunakan bermacam-macam metode enkripsi untuk menjaga data pengguna. Diantara metode tersebut, enkripsi end-to-end menjadi salah satu metode enkripsi yang paling efektif. Enkripsi end-to-end dalam aplikasi chatting memastikan hanya pengirim dan penerima yang dapat membaca isi pesan, menjaga kerahasiaan dari pihak ketiga, termasuk penyedia aplikasi. Setiap pesan dienkripsi dengan kunci unik yang berubah setiap kali pesan dikirim, menggunakan algoritma seperti SHA256 untuk otentikasi, sehingga pesan tidak dapat direplikasi atau diakses tanpa izin [15].



Gambar 2. Enkripsi End to End[15]

Untuk menjamin keamanan keamanan data saat proses enkripsi end-to-end antara pengirim dan penerima terdapat beberapa tahapan penting, pada gambar 2 dijelaskan menganai tahapan dalam enkripsi end-to-end yang dimulai dari pembuatan kunci enkripsi dan dekripsi yang kuat, pertukaran kunci secara aman menggunakan protokol seperti Diffie-Hellman, enkripsi pesan oleh pengirim, pengiriman pesan melalui jaringan, dekripsi pesan oleh penerima, dan verifikasi dan autentikasi untuk memastikan pesan berasal dari pengirim yang sah.

Dalam konteks penelitian ini, enkripsi end-to-end digunakan untuk melindungi data di iCloud, untuk memastikan bahwa hanya pengguna yang dapat melihatnya dan mencegah pihak ketiga dan juga penyedia layanan dapat melihatnya. Proses ini melibatkan enkripsi data sebelum dikirim ke server iCloud dan hanya dapat dekripsi oleh perangkat pengguna, sehingga hal ini dapat memastikan agar data tetap aman saat disimpan dan dikirim.

4) Face ID

Face ID merupakan sebuah metode pengamanan yang menggunakan sistem kamera TrueDepth dan teknologi canggih untuk memetakan wajah pengguna secara akurat dan memberikan otentikasi yang intuitif dan aman. Face ID menggunakan jaringan saraf untuk mendeteksi perhatian, mencocokan wajah, dan mencegah penipuan, sehingga memungkinkan pengguna membuka kunci perangkat mereka hanya dengan pandangan sekilas, bahkan saat memakai masker. Face ID beradaptasi dengan perubahan penampilan pengguna dan secara hati-hati melindungi informasi pribadi dan data biometrik. Saat perangkat aktif, kamera TrueDepth mendeteksi wajah pengguna, mengizinkan akses, kamera TrueDepth mendeteksi wajah pengguna, mengizinkan akses, dan menampilkan pemberitahuan login [16]. Dalam penelitian ini, Face ID digunakan pada iCloud untuk meningkatkan keamanan dan kemudahan pengguna dalam mengakses layanan dan data. Dengan menggunakan Face ID, pengguna dapat membuka kunci akun iCloud, menyinkronkan data, dan mengelola data pribadi mereka dengan lebih mudah dan aman. Teknologi TrueDepth mengurangi resiko akses tidak sah karena hanya pemilik sah yang dapat mengakses akun.

C. Tantangan dan Mitigasi Risiko

Salah satu hal penting yang perlu diperhatikan oleh penyedia layanan cloud yaitu memastikan layanan yang disediakan dapat menjamin ketersediaan dan kemudahan akses data bagi penggunanya. Selain itu, tantangan keamanan data

cloud menjadi fokus utama bagi penyedia layanan yang harus dikelola dengan baik [17]. Oleh karena itu, memahami tantangan-tantangan tersebut sangat penting untuk memastikan data yang tersimpan didalam cloud tetap aman dari ancaman yang ada. Selain itu, diperlukan pula strategi mitigasi risiko yang efektif untuk mengatasi potensi permasalahan yang ada. Berikut ini akan dibahas mengenai beberapa tantangan mengenai keamanan dan privasi data yang dapat timbul pada iCloud, serta langkah-langkah mitigasi yang dilakukan untuk mengatasi potensi resiko tersebut.

a. Ancaman Keamanan Siber

Dalam layanan cloud, keamanan data dari segala ancaman baik dari dalam maupun luar (eksternal) seperti peretasan, phising, ataupun malware menjadi hal yang sangat penting untuk diperhatikan. Maka dari itu diperlukan upaya pencegahan terhadap serangan tersebut, salah satu upaya untuk menghadapi masalah ini yaitu dengan melakukan pengamanan digital (cyber security). Menurut Rahmawati C. (2019), sesuai dengan definisinya, cyber security diartikan sebagai kegiatan pencegahan dan pengamanan sumber daya telematika agar tidak terjadi kejahatan (cybercrime) di dunia siber. Keamanan siber juga dapat diartikan sebagai upaya untuk mencegah serangan di dunia siber[18].

Dalam konteks ini, layanan iCloud memberikan berbagai lapisan perlindungan untuk melindungi data pengguna dari ancaman keamanan siber. Salah satu upaya yang dilakukan oleh Apple yaitu dengan menerapkan enkripsi data seperti enkripsi saat data saat transit dan saat tersimpan di dalam server dengan enkripsi AES ataupun enkripsi end-to-end yang digunakan untuk melindungi data seperti pesan, foto, dan catatan yang menjamin hak akses data hanya diberikan pada perangkat yang terpercaya saja. Dan juga, Apple menawarkan fitur perlindungan data lanjutan, untuk meningkatkan jumlah kategori data yang dilindungi dengan enkripsi end-to-end.

b. Akses dan Transfer Data

Pada saat proses pengaksesan dan transfer data, diperlukan suatu cara pengamanan dari ancaman pihak luar karena dalam proses perpindahan data tersebut memungkinkan terjadinya kebocoran data dan pencurian data. Jika data tidak dilindungi dengan baik, pihak ketiga dapat mengintervensi proses transfer data antara cloud dan perangkat. Salah satu metode yang digunakan oleh Apple pada layanan iCloud untuk mengatasi masalah ini yaitu dengan menggunakan metode TLS atau Transport Layer Security untuk melindungi data selama transfer antara perangkat dan server iCloud. Transport Layer Security (TLS) berfungsi untuk memastikan bahwa data yang dikirimkan tidak dapat diakses atau diubah oleh pihak ketiga selama proses transfer data ke dalam server.

c. Kecerobohan Pengguna

Selain kelemahan dan kesalahan pada sistem layanan iCloud, tak jarang juga terjadi kecerobohan yang dilakukan oleh user itu sendiri. Salah satu nya yaitu saat pengguna kehilangan perangkat mereka yang mengakibatkan data yang ada di dalamnya dapat diakses atau pun dicuri oleh orang yang tidak sah atau kemungkinan terburuknya data tersebut akan disalahgunakan. Dalam menangani hal tersebut, Apple telah memberikan langkah yang dapat digunakan pengguna untuk pencegahan data diakses oleh orang lain. Apple menawarkan fitur untuk menyinkronkan data antar perangkat dan memungkinkan pengguna mengunci perangkat mereka saat hilang, sehingga hal ini dapat membantu mencegah akses tidak sah ke data jika perangkat jatuh ke tangan yang salah.

d. Kesalahan Konfigurasi

Selain kecerobohan kehilangan perangkat, terkadang pengguna juga melakukan dapat melakukan kesalahan dalam konfigurasi salah satunya yaitu kecerobohan karena tidak mengingat ataupun menyimpan konfigurasi password milik pribadi. Dengan konfigurasi yang tidak tepat, hal tersebut dapat beresiko untuk terbukanya celah keamanan oleh pihak yang tidak bertanggung jawab.

Menurut OWASP, Kesalahan konfigurasi dapat menyebabkan aplikasi terbuka untuk diserang. Contoh umum dari kesalahan konfigurasi termasuk penggunaan kata sandi default, kebijakan kata sandi yang tidak aman, perangkat lunak yang tidak diperbarui, dan direktori yang tidak dilindungi. Langkah pencegahan termasuk audit keamanan

secara teratur dan memastikan semua pengaturan keamanan diperbarui sesuai standar [19].

Dalam mengatasi hal ini, selain melakukan audit keamanan secara teratur untuk memastikan bahwa konfigurasi tetap aman, Apple juga menawarkan panduan dan pengaturan default yang aman untuk pengguna. Penggunaan fitur reset password yang aman membantu pengguna dalam mengatasi masalah akses tanpa khawatir tentang adanya gangguan atau pelanggaran keamanan.

e. Resiko Kehilangan Data

Mencadangkan data merupakan salah satu suatu kegiatan yang seharusnya dilakukan oleh pengguna, apalagi bagi seseorang yang sering memiliki data penting yang tersimpan pada perangkat mereka. Ketika pengguna tidak rutin melakukan pencadangan data mereka, hal tersebut akan mengakibatkan resiko kehilangan data penting yang belum sempat tersimpan apa lagi bila terjadi insiden seperti kerusakan perangkat, kehilangan perangkat ataupun serangan malware yang mengakibatkan data hilang.

Dalam mengatasi hal ini, Apple mengambil beberapa langkah mitigasi yang mencakup fitur pencadangan otomatis pada iCloud, yang secara otomatis akan mencadangkan data pengguna setiap kali perangkat mereka terhubung dengan jaringan seperti wifi contohnya. Selain itu Apple juga menggunakan notifikasi untuk mengingatkan pengguna agar segera melakukan pencadangan atau memperbaiki masalah yang menghalangi proses pencadangan tersebut, contohnya apabila koneksi dengan internet terputus. Apple juga memberikan pembaruan atau perbaikan software secara berkala terhadap keamanan dan bug untuk memastikan perangkat selalu terlindungi dan berfungsi secara optimal. Dengan langkah-langkah tersebut, Apple berusaha untuk mengurangi resiko kehilangan data dan menjamin keamanan serta kenyamanan pengguna iCloud.

IV. KESIMPULAN

Berdasarkan analisis yang telah dilakukan, dapat disimpulkan bahwa Apple menunjukkan perhatian yang besar dan berkomitmen untuk menjaga keamanan dan privasi data pengguna dengan menerapkan berbagai mekanisme keamanan seperti, autentikasi dua faktor, enkripsi data end-to-end, AES, dan aturan ketat terhadap aplikasi pihak ketiga, sehingga membuat data pengguna dalam layanan Apple iCloud dapat terlindungi dari berbagai ancaman. Meskipun demikian, penting bagi pengguna untuk tetap berhati-hati dan mengikut protokol keamanan yang tepat untuk melindungi akun dari potensi ancaman.

REFERENSI

[1] Z. Masyhur, A. Rizaldy, P. Kartini, and D. Publikasi, "Studi Literatur Keamanan dan Privasi Data Sistem Cloud Computing Pada Platform Google Drive," 2021.

[2] Agus Irawan, Destiawati Fitriana, and Dhika Harry, "Perbandingan Cloud Computing Micosoft Onedrive, Dropbox, dan Google Drive," Faktor Exacta, vol. 12, no. 1, p. 1, May 2019, doi: 10.30998/faktorexacta.v12i1.3458.

[3] Institute of Electrical and Electronics Engineers, 2019 IEEE 4th International Conference on Computer and Communication Systems : ICCCS 2019 : February 23-25, 2019, Singapore.

[4] O. Toxirjonovich, A. Zaylobiddinovich, and A. Vohidjon O'g'li, "An Overview Of Anomaly Detection Systems In Cloud Networks And An Overview Of Security Measures In Cloud Storage," The American Journal of Engineering and Technology , vol. 03, no. 02–2021, pp. 140–157, 2021.

[5] W. Andriani, "Penggunaan Metode Sistematik Literatur Review dalam Penelitian Ilmu Sosiologi," Jurnal PTK dan Pendidikan, vol. 7, no. 2, Jan. 2022, doi: 10.18592/ptk.v7i2.5632.

[6] Apple, "iCloud data security overview." Accessed: Jun. 18, 2024. [Online]. Available: https://support.apple.com/en-us/102651

[7] S. Sun, H. Ma, Z. Song, and R. Zhang, "WebCloud: Web-Based Cloud Storage for Secure Data Sharing Across Platforms," IEEE Trans Dependable Secure Comput, vol. 19, no. 3, pp. 1871–1884, 2022, doi: 10.1109/TDSC.2020.3040784.

[8] A. Inc, "Keamanan Platform Apple," 2022.

[9] J. Satrio, S. Maryam, A. Ummah, and D. Tri Saputra Wahidin, "Peningkatan Keterampilan Keamanan Siber bagi Pengelola Situs Desa Baros Kabupaten Serang," Jurnal Inovasi Pengabdian dan Pemberdayaan Masyarakat, vol. 2, no. 2, pp. 135–142, Nov. 2022, doi: 10.54082/jippm.35.

[10] K. M. Fitria, "ANALISIS SERANGAN MALWARE DALAM PERBANKAN DAN PERENCANAAN SOLUSI KEAMANAN," Jurnal Informatika dan Teknik Elektro Terapan, vol. 11, no. 3, Aug. 2023, doi: 10.23960/jitet.v11i3.3312.

[11] I. Ali, "Examining cyber security implementation through TLS/SSL on academic institutional repository in Indonesia," Berkala Ilmu Perpustakaan dan Informasi, vol. 17, no. 2, pp. 238–249, 2021, doi: 10.22146/bip.v17i1.2082.

[12] K. I. Santoso, M. A. Muin, and M. A. Mahmudi, "Implementation of AES cryptography and twofish hybrid algorithms for cloud," in Journal of Physics: Conference Series, Institute of Physics Publishing, May 2020. doi: 10.1088/1742-6596/1517/1/012099.

[13] Wahyudi, "Penerapan Metode Advanced Encryption Standard (AES) Pada Keamanan Password Server Cloud Universitas Budi Darma," Nasional Teknologi Informasi dan Komputer), vol. 6, no. 1, 2022, doi: 10.30865/komik.v6i1.5769.

[14] M. Ridhoi, "SKRIPSI IMPLEMENTASI ALGORITMA ELLIPTIC CURVE CRYPTOGRAPHY (ECC) DENGAN END-TO-END ENCRYPTION PADA APLIKASI CHAT BERBASIS MOBILE Disusun dan diajukan oleh: MUHAMMAD RIDHOI D121 18 1303 PROGRAM STUDI SARJANA TEKNIK INFORMATIKA FAKULTAS TEKNIK UNIVERSITAS HASANUDDIN GOWA 2023," 2023.

[15] I. Juniarmi, “Analisis Keamanan Data pada Aplikasi Chatting Menggunakan Enkripsi End-to-End,” Technologia Journal: Jurnal Informatika, vol. 1, no. 2, pp. 3046–9163, 2024, doi: 10.62872/ppr42775.
[16] E. Bratli, R. Endré Dahl, and H. Meling, “Document Verification System on iOS with Face ID/Touch ID.”
[17] Maniah, E. Abdurachman, F. L. Gaol, and B. Soewito, “Survey on threats and risks in the cloud computing environment,” in Procedia Computer Science, Elsevier B.V., 2019, pp. 1325–1332. doi: 10.1016/j.procs.2019.11.248.
[18] C. Rahmawati, “Tantangan Dan Ancaman Keamanan Siber Indonesia Di Era Revolusi Industri 4.0,” Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO AAU), vol. 1, no. 1, pp. 299–306, 2019.
[19] OWASP, “Security Misconfiguration.” Accessed: Jun. 09, 2024. [Online]. Available: https://owasp.org/Top10/A05_2021-Security_Misconfiguration/.