Jurnal Teknik Informatika (JUTIF)
Vol. 4, No. 2, April 2023, hlm. 279-290

DOI: https://doi.org/10.52436/1.jutif.2023.4.2.744
p-ISSN: 2723-3863
e-ISSN: 2723-3871

CRYPTOGRAPHIC PROTOCOL SECURITY IN NATIONAL ENCRYPTION APPLICATIONS

Agung Widodo[*1], Yohan Suryanto[2]

[1,2]Departemen Teknik Elektro Universitas Indonesia, Indonesia
Email: [1] agung.widodo01@ui.ac.id, [2]yohan.suryanto@ui.ac.id

(Naskah masuk: 11 Desember 2022, Revisi : 03 Januari 2023, diterbitkan: 23 Maret 2023)

Abstract

In the era of digital transformation, information exchange, especially confidential and strategic information has become the most vital aspect for almost all organizations. Various bad precedents regarding classified and strategic information leaks in Indonesia have become a slap in the face that must be acknowledge and answered with effective solutions. In 2020, XYZ Agency developed a file encryption application (ABC Application) to address the challenge of securing confidential information, especially those transmitted on electronic channels. Until 2022, the ABC Application has been implemented in a limited scope and its implementation is planned to be expanded nationally. After 2 years of operation, the XYZ Agency has conducted a study on the security of the algorithm used in ABC Application, but unfortunately has not conducted an in-depth study regarding the security of the protocol suite used in the Application. In this research, a security analysis of ABC application protocol suites, namely the registration protocol, user verification, key generation, and key request for the encryption-decryption process protocol was conducted through formal verification approach using the Scyther Tool. The analysis focuses on aspects of guaranteeing confidentiality of information and authentication with four criteria, namely secrecy, aliveness, synchronization, and agreement. The experimental results showed that these protocols meet the security criteria for the transmitted confidential information but have general weaknesses in the authentication aspect, especially for synchronization and agreement criteria. Based on these weaknesses, technical recommendations are proposed that are able to overcome the identified weaknesses.

Keywords: *ABC Application, Confidential Information, Cryptographic Protocol, Scyther Tool.*

KEAMANAN PROTOKOL KRIPTOGRAFI PADA APLIKASI ENKRIPSI NASIONAL

Abstrak

Memasuki era transformasi digital, pertukaraan informasi menjadi aspek paling vital bagi hampir seluruh organisasi, terlebih lagi informasi rahasia dan strategis. Beragam preseden buruk tentang kebocoran informasi rahasia dan strategis di Indonesia menjadi tamparan keras yang harus dijawab dengan solusi efektif. Instansi XYZ telah mengembangkan aplikasi enkripsi file ABC pada tahun 2020 untuk menjawab tantangan pengamanan informasi rahasia khususnya yang ditransmisikan pada kanal elektronik. Hingga tahun 2022, aplikasi ABC telah diimplementasikan secara terbatas dan rencananya, skala implementasi akan diperluas secara nasional. Selang 2 tahun masa operasional, Instansi XYZ telah melakukan kajian terhadap keamanan algoritma yang digunakan dalam Aplikasi ABC, namun belum melakukan kajian mendalam terhadap keamanan rangkaian protokol yang digunakan dalam Aplikasi tersebut. Pada peneitian ini dilakukan analisis keamanan protokol registrasi, verifikasi pengguna, pembangkitan kunci, dan permintaan kunci untuk proses enkripsi-dekripsi Aplikasi ABC dengan pendekatan verifikasi formal menggunakan Scyther Tool. Analisis berfokus pada aspek jaminan kerahasiaan informasi dan autentikasi dengan empat kriteria yaitu *secrecy*, *aliveness*, *synchronization*, dan *agreement*. Hasil percobaan menunjukkan bahwa protokol-protokol tersebut telah menenuhi kriteria *secrecy* untuk informasi rahasia yang ditransmisikan, namun memiliki kelemahan umum pada pada autentikasi khususnya untuk kriteria *synchronization* dan *agreement*. Berdasarkan kelemahan tersebut, diajukan rekomendasi teknis yang mampu mengatasi kelemahan-kelemahan yang teridentifikasi

Kata kunci: *Aplikasi ABC, Informasi Rahasia, Protokol Kriptografi, Scyther Tool*.

1. PENDAHULUAN

Memasuki era transformasi digital, pertukaran informasi menjadi aspek paling vital bagi hampir seluruh organisasi, baik profit maupun non profit yang memanfaatkan teknologi informasi dalam proses bisnisnya. Dengan demikian, informasi menjadi sumber daya vital yang perlu dimanfaatkan dan dilindungi untuk mendukung perkembangan dan keberlanjutan organisasi [1]. Mengetahui hal tersebut, sejalan dengan perspektif manajemen informasi, kepemilikan informasi menjadi hal relevan yang mendasar dalam proses bisnis informasi [2].

Informasi umumnya diklasifikasikan dalam beberapa tingkatan. Secara umum informasi diklasifikasikan menjadi dua, yaitu informasi biasa dan informasi rahasia [2]. Di Indonesia, merujuk Undang-Undang nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (UU KIP) diatur tentang informasi yang dikecualikan. Berdasarkan Pasal 2 UU KIP, informasi terbagi dalam informasi publik dan informasi yang dikecualikan [3]. Merujuk pasal 17 UU KIP, informasi yang dikecualikan dapat dimaknai sebagai informasi yang strategis dan rahasia (sampai dengan titik tertentu). Penanganan terhadap informasi rahasia harus dilakukan dengan tepat sehingga dapat menjamin kerahasiaan informasi tersebut terutama pada tahap diseminasi.

Diseminasi informasi adalah satu tahapan yang vital dalam proses pemanfaatan informasi. Tujuan diseminasi informasi tidak lain adalah mengkomunikasikan suatu informasi dari pembuat informasi kepada para pihak yang membutuhkan. Banyak pakar dari lintas disiplin ilmu menegaskan bahwa komunikasi adalah cara bagaimana suatu organisasi baik secara internal maupun eksternal melakukan interaksi berkelanjutan [4].

Melihat tingginya nilai substansi komunikasi yang melibatkan informasi rahasia maka komunikasi rahasia selalu menjadi target serangan [5]. Hal ini menjadi ancaman karena apabila konten dari komunikasi rahasia bocor maka dapat menimbulkan risiko terhadap pemilik informasi dan *stakeholder* yang terlibat dengan informasi tersebut [5]. Beberapa kejadian mengenai serangan terhadap komunikasi rahasia di Indonesia di antaranya penyadapan percakapan Presiden Susilo Bambang Yudhoyono melalui jaringan Selular di Cikeas pada November 2013 yang dilakukan oleh pihak kedutaan besar Australia dengan memasang alat penyadap yang dipasang di *base station* terdekat [6], [7]. Kasus dugaan penyadapan rumah dinas Presiden Jokowi, juga dapat menjadi preseden sebagaimana disampaikan oleh Sekretaris Jendral Partai Demokrat Indonesia Perjuangan, Tjahjo Kumolo pada Februari 2014 silam [8].

Dalam konteks spesifik, informasi yang berkaitan dengan data dukung untuk audit keamanan siber suatu organisasi, terutama organisasi yang termasuk dalam Infrastruktur Informasi Vital [9], [10]. Pasalnya, jika diolah oleh pihak yang tidak berwenang, informasi tersebut dapat memberikan gambaran terhadap celah keamanan bagi organisasi tersebut [5], [9]. Di Indonesia, khususnya untuk sektor pemerintah, Instansi yang berwenang dalam melakukan audit keamanan siber adalah Instansi XYZ. Kewenangan ini dinyatakan dalam Peraturan Instansi XYZ. Dalam peraturan tersebut, Instansi XZY mengatur tentang ketentuan sistem pengamanan dalam penyelenggaraan sistem elektronik melalui penilaian indeks keamanan informasi untuk berbagai organisasi termasuk Infrastruktur Informasi Vital [9], [10].

Kebocoran informasi adalah hal yang tidak boleh terjadi. Sebagai upaya antisipasi atas kebocoran informasi, maka Instansi XYZ aplikasi enkripsi *file* (Aplikasi ABC) untuk menjamin kerahasiaan informasi terkait audit keamanan siber yang diserahterimakan antara Instansi XYZ dengan organisasi pemangku kepentingan selama proses audit berlangsung. Aplikasi ABC merupakan aplikasi pengamanan *file* digital melalui teknik enkripsi yang dikembangkan oleh Instansi XYZ pada tahun 2021.

Aplikasi ABC digunakan untuk kebutuhan kirim terima dokumen rahasia. Keamanan informasi dalam proses tersebut berfokus pada kerahasiaan, keutuhan dan ketersediaan informasi [12]–[15]. Untuk memberikan jaminan kerahasiaan informasi, Aplikasi ABC menerapkan teknik-teknik kriptografi seperti enkripsi dan fungsi *hash* [16]. Karena pentingnya peran Aplikasi ABC, dalam proses pelaksanaan penjaminan informasi audit, maka kemampuan Aplikasi ABC untuk memberikan jaminan keamanan informasi harus dipastikan. Untuk mengetahui kemampuan Aplikasi ABC dalam mengamankan informasi, perlu dilakukan analisis keamanan. Untuk komunikasi rahasia, analisis keamanan kriptografi terhadap algoritma dan protokol komunikasi adalah pendekatan yang paling relevan untuk menguji apakah fitur keamanan yang diberikan oleh Aplikasi ABC sudah sesuai dengan yang diharapkan [17], [18]. Pembuktian ini tidak hanya penting untuk mengakomodasi keperluan teknis akademis saja, namun ke depannya juga diharapkan dapat menjadi penguat untuk menjawab tantangan perlindungan data pribadi pasca diundangkannya Undang-Undang Nomor 27 tahun 2022 tentang Pelindungan Data Pribadi [19].

Menurut hasil wawancara, Aplikasi ABC telah digunakan untuk mengenkripsi *file* rahasia dalam proses audit keamanan siber. Berselang hampir satu tahun operasional, belum pernah dilakukan kajian keamanan protokol kriptografi yang ada pada Aplikasi ABC. Analisis keamanan protokol kriptografi biasanya berfokus dengan fitur kriptografi yang digunakan untuk menjamin keamanan baik kerahasiaan dan keutuhan informasi yang ditransmisikan serta kriteria nir-penyangkalan dan autentikasi dari pihak-pihak yang terlibat dalam komunikasi [18], [20] – [22]. Beberapa peneliti di lima tahun terakhir banyak yang lebih berfokus pada penelitian terkait protokol autentikasi mengingat

aspek autentikasi termasuk "rentan" akibat kelalaian desain protokol ataupun kurangnya mekanisme pengamanan [23]–[26]. Selain itu, *adversary model* untuk protokol autentikasi juga banyak berkembang [27].

Dari penelitian-penelitian terdahulu, umumnya, dapat diketahui bahwa terdapat dua pendekatan analisis protokol kriptografi yaitu melalui verifikasi formal dan pengamatan langsung, baik dengan menggunakan alat bantu, maupun tidak [28], [29]. Salah satu alat bantu verifikasi formal protokol kriptografi yang popular adalah Scyther Tool [30]. Dalam 5 tahun terakhir Scyther banyak digunakan untuk melakukan pengujian terhadap aspek autentikasi dan kerahasiaan pada protokol-protokol baru [33]–[37]. Penelitian-penelitian tersebut sebagian besar memiliki fokus penelitian yang sama, yaitu pada bagaimana cara membuktikan keandalan sebuah protokol kriptografi dalam aspek keamanananya. Metode penelitian yang dilakukan pun sama, yaitu melalui pemodelan, pengujian, analisis, dan pemberian rekomendasi. Hal yang membedakan antara penelitian satu dengan penelitian lainnya adalah objek. Seperti halnya protokol transaksi pada [31] dan [37], protokol komunikasi berbasis *password* pada [32], protokol 5G-AKA berbasis kunci simetris [33], protokol pemindahan kepemilikan pada [34], serta protokol autentikasi dan penetapan kunci pada [35] dan [36]. Perbedaan penelitian ini dengan penelitian-penelitian lainnya adalah terletak pada objek penelitian yang berfokus pada 5 protokol yang tergabung dalam paket protokol pada Aplikasi ABC. Yang membuat penelitian ini lebih unik adalah fakta bahwa objek penelitian ini merupakan objek yang bersifat strategis.

Berdasarkan elaborasi urgensi tersebut, tujuan dari penelitian ini adalah untuk membuktikan keandalan paket protokol Aplikasi ABC melalui analisis keamanan terhadap protokol registrasi, verifikasi pengguna, pembangkitan kunci asimetrik, dan permintaan kunci enkripsi-dekripsi Aplikasi ABC. Hasil dari penelitian ini diharapkan dapat menjadi pelengkap kajian keamanan pada salah satu aplikasi pendukung komunikasi rahasia di Indonesia menggunakan metode verifikasi formal dengan *Scyther* sebagai alat bantunya.

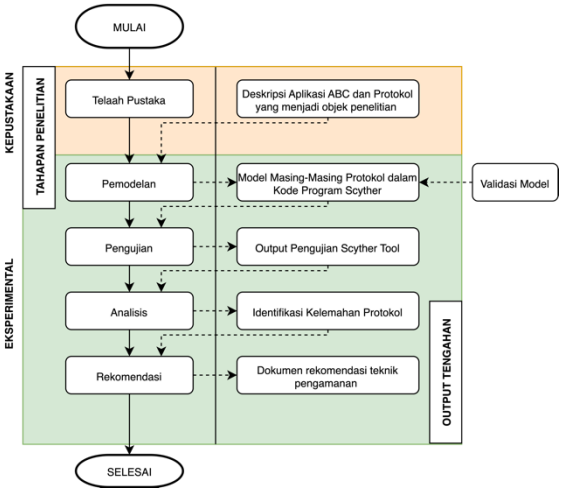
2. METODE PENELITIAN

Penelitian dilaksanakan dengan tahapan seperti diilustrasikan pada Gambar 1. Secara keseluruhan, penelitian ini menggunakan dua metode, yaitu metode kepustakaan dan eksperimen. Dua metode tersebut dijabarkan dalam lima tahapan dengan lima buah *output* tengahan. *Output* tengahan dari setiap tahapan menjadi *input* bagi tahap berikutnya.

Metode kepustakaan memiliki satu tahapan, yaitu telaah pustaka. Tahap ini digunakan untuk menghasilkan Deskripsi Aplikasi ABC dan protokol yang menjadi objek penelitian. Dokumen yang diproses pada tahap ini adalah:

1. Pada tahap pemodelan, dilakukan Petunjuk Teknik Aplikasi ABC; dan
2. Dokumentasi Spesifikasi Teknis Protokol Kriptografi Aplikasi ABC.

pembuatan model protokol dalam bentuk kode program *Scyther*. Model tersebut merupakan input untuk *Scyther* dalam melakukan pengujian. Hasil pengujian kemudian dianalisis sesuai dengan teori keamanan informasi dan kriptografi. Daftar kelemahan yang teridentifikasi berdasarkan hasil analisis kemudian digunakan sebagai dasar perumusan rekomendasi teknik-teknik pengamanan untuk memperbaiki protokol.



Gambar 1. Alur Penelitian
Sumber: diolah secara mandiri.

3. HASIL DAN PEMBAHASAN

3.1. Gambaran Umum dan Arsitektur Aplikasi ABC

Aplikasi ABC adalah aplikasi pengamanan *file* yang dikembangkan oleh Instansi XYZ. Aplikasi ini dapat digunakan pada perangkat *Personal Computer* (PC) atau laptop dengan sistem operasi Windows.

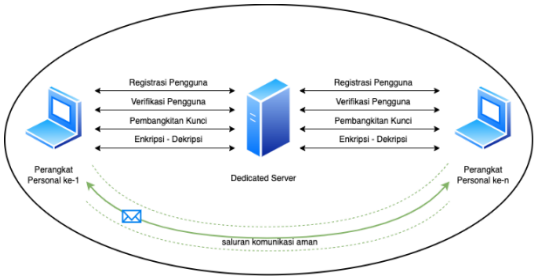
Arsitektur yang digunakan adalah *client-server*, yaitu untuk dapat melakukan fungsinya Aplikasi ABC perlu terhubung dengan *server*. *Server* yang digunakan berfungsi sebagai pengelolaan pengguna dan manajemen kunci terpusat.

Seluruh perangkat yang terkoneksi menggunakan Aplikasi ABC berkomunikasi dengan *server* ini untuk menyelesaikan tahapan registrasi, verifikasi pengguna, pembangkitan kunci publik digunakan untuk melakukan enkripsi *file* khusus untuk penerima yang dituju.

Pada proses pengamanan *file* yang dilakukan oleh aplikasi ABC menggunakan algoritma simetrik untuk proses enkripsinya. Sedangkan untuk proses pengiriman kunci enkripsi dan dekripsi dari *server* ke aplikasi desktop menggunakan infrastruktur kunci publik.

Pada penggunaan aplikasi ABC versi 2 terdapat 2 kategori pengguna, yaitu administrator dan

operator. Pengguna administrator adalah pengelola aplikasi yang dapat melakukan proses administrasi aplikasi ke *server*. Proses administrasi yang bisa dilakukan di antaranya pendaftaran pengguna, blokir pengguna dan pengecekan log. Pada mode operator yang merupakan operasional dari aplikasi ABC. Operator dapat menggunakan aplikasi ABC untuk registrasi pengguna, *login* pengguna, pembangkitan kunci asimetrik, pembangkitan kunci enkripsi, pembukaan kunci dekripsi. Adapun arsitektur Aplikasi ABC digambarkan pada Gambar 2.



Gambar 2. Arsitektur Sistem Aplikasi ABC
Sumber: diolah secara mandiri berdasarkan [16]

Proses kirim terima dokumen yang telah dienkripsi tidak diakomodasi dalam aplikasi, melainkan menggunakan saluran komunikasi aman lain. Saluran tersebut beragam dapat berupa saluran *mobile-based* atau *web-based*..

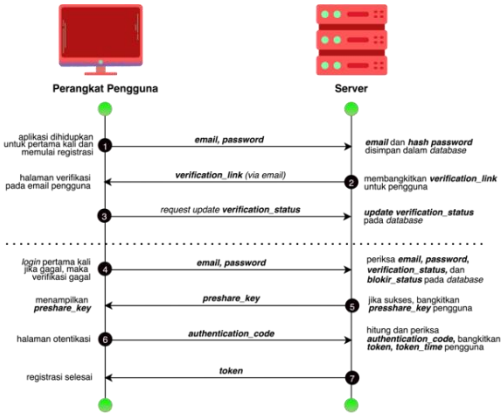
3.2. Protokol Kriptografi pada Aplikasi ABC

Aplikasi ABC memiliki lima protokol yang mendukung proses bisnis aplikasi, yaitu protokol registrasi pengguna, verifikasi pengguna, pembangkitan kunci asimetrik, permintaan kunci enkripsi, dan permintaan kunci dekripsi. Masing-masing protokol akan dijelaskan secara berurutan.

3.2.1. Protokol Registrasi Pengguna

Protokol registrasi pengguna merupakan protokol yang digunakan pada proses pendaftaran pengguna agar dapat menggunakan fungsi dari Aplikasi ABC. Pendaftaran pengguna dilakukan dengan mendaftarkan *email* dan *password* yang digunakan untuk *login* ke Aplikasi ABC. Selain itu juga terdapat proses pengaturan *Two Factor Aunthetication*. Proses protokol registrasi pengguna dapat dilihat pada Gambar 3

Proses protokol ABC dimulai ketika *user* pertama kali masuk ke dalam aplikasi akan diminta untuk mengisi *email*, *password* dan validasi *password*. Setelah *user* mengisi form yang telah diberikan oleh aplikasi, maka *server* akan menyimpan email dan hasil hash dari *password* ke dalam *database server*. Selanjutnya, *server* membangkitkan *link* verifikasi yang akan dikirimkan untuk *user*. Proses pengiriman *link* verifikasi tersebut akan dikirimkan melalui *email*.



Gambar 3. Protokol Registrasi Pengguna Aplikasi ABC
Sumber: diolah secara mandiri berdasarkan [16]

Ketika *link* verifikasi tersebut sudah diakses oleh *user*, maka akan muncul halaman untuk melakukan verifikasi. Setelah *user* meng-klik *link* verifikasi, maka *user* akan mengirimkan update verification_status ke *server*. Setelah itu, nilai verification_status yang ada di *database* akan terupdate. Setelah terverifikasi, maka email dan *password* yang telah didaftarkan dapat digunakan ketika proses login.

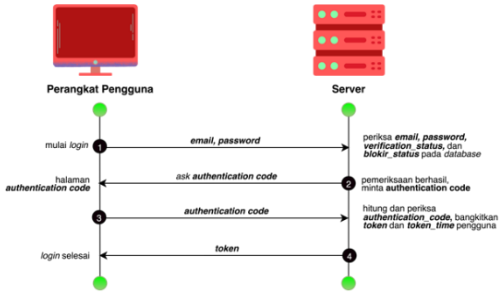
Pada proses *login* pertama kali, *user* mengisi form *email* dan *password* yang telah di registrasi sebelumnya. Selanjutnya, *server* akan melakukan pengecekan *email*, nilai hash *password*, status verifikasi, dan status blokir yang ada di dalam *database server*. Apabila status verifikasi masih belum terverifikasi, maka akan memunculkan notifikasi bahwa akun belum terverifikasi. Hal tersebut juga berlaku apabila status blokir menunjukkan bahwa akun tersebut terblokir, maka akan memunculkan notifikasi bahwa akun yang diberikan *user* ke *server* telah terblokir sehingga tidak bisa mengakses aplikasi. Apabila akun tersebut telah terverifikasi dan tidak ada status blokir, maka *server* akan membangkitkan *preshared key* untuk *user* yang nantinya akan dikirimkan melalui *Time Based One Time Password* (TOTP).

Setelah *preshared key* dikirimkan oleh *server*, maka akan muncul halaman untuk melakukan autentikasi dengan menggunakan *preshared key* yang telah dikirimkan sebelumnya. Proses autentikasi dilakukan dengan cara *user* akan mengirimkan kode autentikasi ke *server*. Selanjutnya, *server* akan mengecek kode autentikasi tersebut apakah sudah sesuai atau belum. Apabila telah sesuai, maka *server* akan mengirimkan *token* dan *token_time* untuk jangka waktu dari *token* tersebut. Selanjutnya, *token* dan *token_time* akan dikirimkan ke *user* dan *user* dapat masuk ke dalam aplikasi dengan sesi dari *token* yang telah dikirim oleh *server*.

3.2.2. Protokol Verifikasi Pengguna

Protokol verifikasi pengguna merupakan proses autentikasi yang dilakukan oleh aplikasi dan *server* sebelum *user* dapat menggunakan layanan aplikasi.

Setelah *user* melakukan registrasi di dalam *server*, selanjutnya *user* dapat melakukan *login* untuk dapat masuk ke dalam aplikasi. Proses protokol verifikasi pengguna dapat dilihat pada Gambar 4.



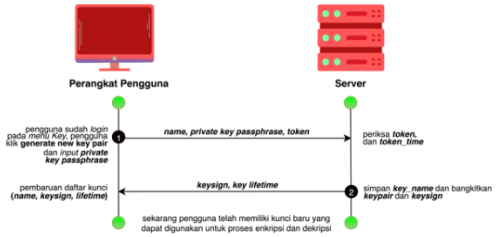
Gambar 4. Protokol Verifikasi Pengguna Aplikasi ABC
Sumber: diolah secara mandiri berdasarkan [16]

Proses protokol ABC dimulai ketika *user* membuka aplikasi, aplikasi akan memberikan form *email* dan *password* yang nantinya akan diisi oleh *user* sesuai dengan *email* dan *password* yang telah diregistrasi sebelumnya. Setelah *user* mengisi form, maka *email* dan *password* tersebut akan dikirimkan ke *server* untuk melakukan pengecekan *email*, *password*, status verifikasi, dan status blokir. Apabila status verifikasi dari *email* dan *password* tersebut belum diverifikasi, maka akan memunculkan notifikasi untuk melakukan verifikasi *email*. Selain itu, apabila status blokir dari email dan *password* tersebut menyatakan bahwa email dan *password* tersebut telah terblokir, maka akan memunculkan notifikasi bahwa email dan *password* tersebut telah terblokir. Apabila status verifikasi telah valid dan status blokir menunjukkan bahwa email dan *password* tersebut tidak diblokir, maka nantinya *server* akan mengirimkan kode autentikasi untuk dikirimkan melalui TOTP.

Setelah *user* mengisi kode autentikasi dari TOTP, selanjutnya aplikasi akan mengirimkan kode autentikasi tersebut kepada *server* untuk dilakukan pengecekan terhadap kode autentikasi. Apabila kode autentikasi yang dikirimkan oleh *user* tersebut benar, maka *server* akan membangkitkan *token* dan *token_time* untuk *user* dapat masuk kedalam sesi aplikasi. Setelah *token* dan *token_time* dikirimkan oleh *server* kepada *user*, maka *user* dapat mengakses fitur aplikasi dengan jangka waktu sesuai dengan pengaturan waktu sesi yang ada di dalam *token*_time..

3.2.3. Protokol Pembangkitan Kunci Asimetrik

Protokol pembangkitan kunci asimetrik merupakan proses pembangkitan pasangan kunci asimetrik, *user* akan membuat pasangan kunci yang diperlukan untuk proses enkripsi dan dekripsi *file* yang membutuhkan kunci dalam prosesnya. Proses protokol verifikasi pengguna dapat dilihat pada Gambar 5.



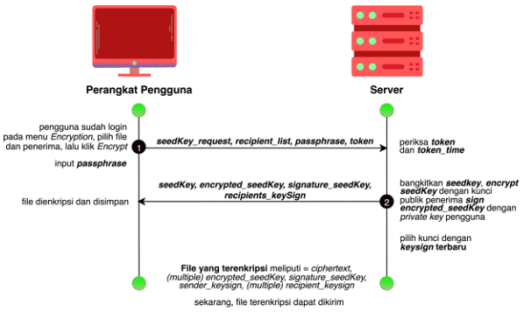
Gambar 5. Protokol Pembangkitan Kunci Aplikasi ABC
Sumber: diolah secara mandiri berdasarkan [16]

User dapat membuat pasangan kunci tersebut di dalam menu kunci dan mengklik tombol bangkitkan pasangan kunci baru. Ketika *user* mengklik tombol tersebut, maka akan muncul *form private key passphrase*. *Passphrase* ini dibutuhkan oleh *user* untuk melakukan dekripsi *file* yang dikirim oleh pengirim ke *user*. Selanjutnya, *user* akan mengirimkan nama *user*, *private key passphrase*, dan *token* untuk dikirimkan kepada *server*. *Server* akan mengecek validitas dari *token* dan *token*_time. Apabila valid, maka *server* akan menyimpan nama dan membangkitkan pasangan kunci dan *keysign*.

Selanjutnya, pasangan kunci dan *keysign* tersebut nantinya akan disimpan di dalam *database* milik *server*. Setelah pasangan kunci dan *keysign* tersebut disimpan di dalam *database* milik *server*, *keysign* dan *key lifetime* dari *user* kemudian dikirimkan ke *user* untuk dapat digunakan oleh *user* dalam proses enkripsi dan dekripsi *file* di dalam aplikasi. List kunci yang ada di aplikasi milik *user* juga akan diperbarui dengan informasi terkait nama, *keysign*, dan *key lifetime* dari pasangan kunci yang telah dibangkitkan oleh *user*. Kunci yang telah dibuat merupakan kunci asimetrik yang terdiri dari kunci public dan kunci privat. Kunci publik nantinya akan digunakan selama proses enkripsi *file* dan kunci privat digunakan selama proses dekripsi *file*..

3.2.4. Protokol Permintaan Kunci Enkripsi

Dalam proses enkripsi *file* yang nanti akan dikirimkan *user* ke penerima, diperlukan permintaan kunci untuk melakukan enkripsi *file* tersebut. Hal ini dikarenakan aplikasi yang ada pada *user* tidak menyimpan kunci enkripsi milik penerima sehingga *user* perlu untuk meminta kunci tersebut kepada *server*. Proses protokol permintaan kunci enkripsi digambarkan pada Gambar 6.



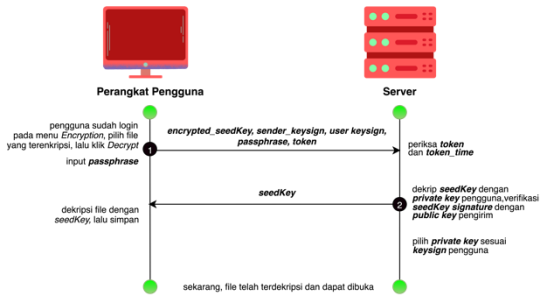
Gambar 6. Protokol Enkripsi Aplikasi ABC
Sumber: diolah secara mandiri berdasarkan [16]

Ketika *user* akan meminta kunci untuk enkripsi *file*, *user* akan mengisi form *passphrase* terlebih dahulu. Hal ini diperlukan sebagai autentikasi yang dibutuhkan oleh *server* dari *user*. Selanjutnya, *user* akan mengirimkan permintaan kunci, list penerima, *passphrase*, dan *token* kepada *server*. *Server* akan melakukan validasi pada *token* untuk mengecek apakah *token* yang dikirimkan sedang aktif atau tidak. Apabila *token* tersebut aktif, maka *server* akan membangkitkan kunci, melakukan enkripsi pada kunci menggunakan kunci publik milik penerima *file*, dan melakukan *signing* pada kunci menggunakan kunci privat milik penerima *file*. Kunci yang telah dienkripsi, serta kunci yang telah di-*signing* selanjutnya akan dikirim ke *user*. Kemudian *user* melakukan enkripsi *file* dengan menggunakan kunci yang telah dikirimkan sebelumnya.

Isi dari *file* yang telah terenkripsi tersebut terdiri dari isi *file* yang dienkripsi, kunci yang terenkripsi, *signature* kunci, *keysign* pengirim, dan *keysign* penerima. Kunci yang terenkripsi dan *keysign* penerima dapat lebih dari satu penerima untuk pengiriman satu *file* dari *user* untuk banyak penerima. Setelah *file* tersebut dienkripsi, maka *file* hasil enkripsi tersebut akan disimpan di *storage* milik *user*. *File* hasil enkripsi tersebut nantinya akan dikirimkan oleh *user* ke penerima melalui platform pengiriman *file* yang tersedia.

3.2.5. Protokol Permintaan Kunci Enkripsi

Dalam proses dekripsi *file* yang akan dilakukan *user* penerima, diperlukan permintaan kunci untuk melakukan dekripsi *file* tersebut. Hal ini dikarenakan aplikasi yang ada pada *user* tidak menyimpan kunci enkripsi milik pengirim sehingga *user* perlu untuk meminta kunci tersebut kepada *server*. Proses protokol permintaan kunci dekripsi digambarkan pada Gambar 7.



Gambar 7. Protokol Dekripsi Aplikasi ABC
Sumber: diolah secara mandiri berdasarkan [16]

Dalam Proses Dekripsi *File*, *user* telah memperoleh *file* yang telah dienkripsi yang dikirimkan oleh pengirim untuk *user*. Ketika *user* melakukan dekripsi *file*, *user* masuk ke dalam aplikasi dan memilih menu dekripsi *file*. *User* kemudian memilih *file* yang akan didekripsi berdasarkan *file* enkripsi yang telah dikirimkan oleh pengirim kepada *user*. Selanjutnya, *user* akan diminta untuk mengisi *passphrase*. *Passphrase* ini diperlukan untuk melakukan validasi terhadap kunci privat yang dimiliki oleh *user*. Apabila passhphrase tersebut tidak sesuai, maka akan muncul notifikasi bahwa *passphrase* yang digunakan salah. Apabila *passphrase* tersebut sesuai, maka nantinya aplikasi akan mengirimkan kunci yang terenkripsi, *keysign* pengirim, *keysign user*, *passphrase*, dan *token* kepada *server*.

Server kemudian akan melakukan validasi terhadap *token* yang dikirimkan oleh *user*. Jika *token* tersebut masih aktif, maka selanjutnya *server* akan mencari *keysign* pengirim melalui *database* yang ada pada *server*. Apabila *keysign* tersebut terdapat di dalam *database* milik *server*, maka kunci yang terenkripsi tersebut akan didekripsi menggunakan kunci privat milik *user*. Kunci privat milik *user* dapat diketahui melalui *keysign* milik *user* yang telah dikirimkan oleh *user* sebelumnya. Selain itu, *server* akan melakukan validasi kunci tersebut dengan menggunakan kunci publik milik pengirim. Apabila kunci tersebut valid, maka kunci yang terenkripsi akan di dekripsi menjadi kunci yang dapat digunakan oleh *user* untuk melakukan dekripsi pada *file* yang akan didekripsi. Kunci tersebut akan dikirimkan oleh *server* kepada *user*. Selanjutnya, *user* akan menggunakan kunci tersebut untuk melakukan dekripsi *file* yang diminta.

Setelah dilakukan dekripsi *file*, maka *file* tersebut akan terbuka dan tersimpan di dalam *storage* milik *user*. Selanjutnya, *user* dapatr mengakses dan melihi isi dari *file* yang dikirimkan oleh pengirim kepada *user*..

3.3. Pemodelan dan Pengujian

Pemodelan protokol-protokol Aplikasi ABC dilakukan dengan menyusun protokol mengikuti ketentuan *Scyther Tool*. Pada setiap protokol terdapat dua entitas, yaitu *user* dan *server*, di mana pada *user* selalu bertindak sebagai inisiator.

Validitas model protokol diuji dengan dua pendekatan, yaitu *component checklist* dan *model checking*. Model protokol pada Aplikasi ABC telah diverifikasi di *Scyther Tool*. Model segera divalidasi dengan keluaran verifikasi protokol berdasarkan pendekatan *model checking*. *Component checklist* dilakukan dengan membuat tabel kontrol sesuai dengan spesifikasi protokol. Hasilnya menunjukkan bahwa model yang dibuat dengan bahasa pemrograman lokal *Scyther Tool* mengikuti spesifikasi protokol registrasi pengguna, verifikasi pengguna, pembangkitan kunci, permintaan kunci enkripsi, dan permintaan kunci dekripsi Aplikasi ABC.

Berdasarkan deskripsi protokol-protokol yang telah dijelaskan. Hanya terdapat dua entitas yaitu perangkat pengguna dan *server*. Perangkat pengguna merupakan inisiator di setiap protokol. Adapun untuk setiap pemodelan yang dibuat, *role*, status dan klaim yang digunakan dapat dilihat pada Tabel 1. Kemudian, pada Tabel 2 menjelaskan istilah-istilah

yang digunakan dalam memodelkan *payload* yang dikomunikasikan dalam protokol.

Tabel 1. Ketentuan Dasar Pemodelan Protokol

Role	**Kode**	**Status**	**Klaim**
perangkat pengguna	*user*	*initiatior*	*alive, niagree, nisynch, secret*
dedicated *server*	*server*	*responder*	*alive, niagree, nisynch, secret*

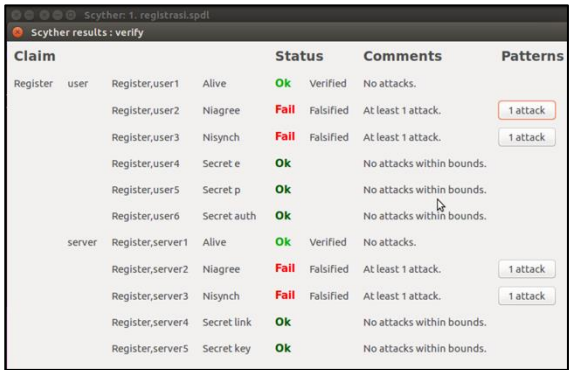
Sumber: diolah secara mandiri berdasarkan [16]

Tabel 2. Pemetaan Istilah-*Payload*

Istilah	***Payload***
e	*email* pengguna
p	*password* pengguna
auth	*authentication code* untuk proses registrasi dan verifikasi pengguna
link	*link* verifikasi *user* baru dari *server* kepada pengguna
key	*preshared key*
token	token sesi akses pengguna
keysign	keterangan penanda unik kunci
keylifetime	keterangan masa berlaku kunci
name	nama pengguna
pass	*passphrase* untuk kunci privat pengguna
seedKey	*seedKey* untuk proses enkripsi-dekripsi

Sumber: diolah secara mandiri berdasarkan [16]

Hasil pengujian kesesuaian untuk kelima protokol ditunjukkan pada Gambar 9, Gambar 10, Gambar 11, Gambar 12, dan Gambar 13 secara berurutan.

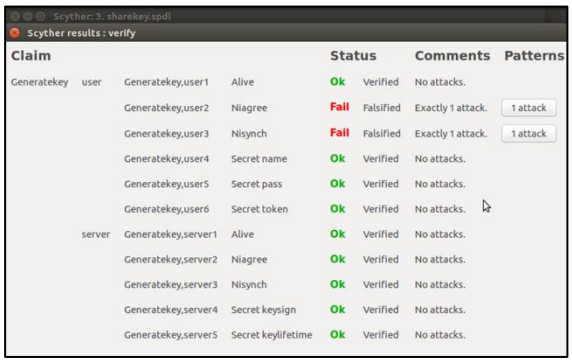


Gambar 9. Hasil Pengujian Protokol Registrasi
Sumber: hasil pengujian pada *Scyther*

Pada pengujian Protokol Registrasi terdapat 4 klaim yang *Fail* (tidak lolos uji) dari 11 klaim, yaitu klaim *niagree* dan *nisynch* pada *role user* maupun *server*.

Gambar 10. Hasil Pengujian Protokol Verifikasi Pengguna
Sumber: hasil pengujian pada *Scyther*

Pada pengujian Protokol Verifikasi Pengguna terdapat 4 klaim yang *Fail* (tidak lolos uji) dari 10 klaim, yaitu klaim *niagree* dan *nisynch* pada *role user* maupun *server*.



Gambar 11. Hasil Pengujian Protokol Pembangkitan Kunci Asimetrik
Sumber: hasil pengujian pada *Scyther*

Pada pengujian Protokol Pembangkitan Kunci Asimetrik terdapat 2 klaim yang *Fail* (tidak lolos uji) dari 11 klaim, yaitu klaim *niagree* dan *nisynch* pada *role user*.

Gambar 12. Hasil Pengujian Protokol Permintaan Kunci Enkripsi
Sumber: hasil pengujian pada *Scyther*

Pada pengujian Protokol Permintaan Kunci Enkripsi terdapat 2 klaim yang *Fail* (tidak lolos uji) dari 8 klaim, yaitu klaim *niagree* dan *nisynch* pada *role user*.

Gambar 13. Hasil Pengujian Protokol Permintaan Kunci Dekripsi
Sumber: hasil pengujian pada *Scyther*

Pada pengujian Protokol Permintaan Kunci Dekripsi, 8 klaim yang diuji OK (lolos uji).

Berdasarkan Gambar 9, Gambar 10, Gambar 11, Gambar 12, dan Gambar 13 dapat diketahui bahwa

terdapat dua aspek yang diuji, yaitu aspek autentikasi dan kerahasiaan. Aspek autentikasi direpresentasikan oleh tiga buah kriteria, yaitu *aliveness, niagree,* dan *nisych*. Sementara aspek kerahasiaan direpresentasikan oleh satu kriteria, yaitu *secret*.

3.4. Analisis

Berdasarkan hasil pengujian, temuan kelemahan protokol-protokol yang diuji diringkas pada Tabel 2.

Secara umum, dari 5 protokol yang diuji, hanya satu protokol yang lolos uji pada seluruh aspek pengujian, yaitu protokol permintaan kunci dekripsi.

Keempat protokol lainnya dinyatakan tidak memenuhi uji. Jika dilihat lebih spesifik, keempat protokol tersebut hanya memiliki masalah pada aspek *authentication* dan tidak memiliki masalah pada aspek *secret*.

Aspek *secret* mengamanatkan agar sebuah protokol mampu menjamin kerahasiaan informasi yang dipertukarkan dalam protokol tersebut. Sementara aspek *authentication* mengamanatkan tiga kriteria yaitu *aliveness*, *synchronization*, *dan agreement*.

Sebuah protokol autentikasi dinyatakan menjamin *aliveness* atau kelangsungan hidup entitas *user* jika entitas lain yang berkomunikasi dengan *user*, yaitu *server*, dapat memastikan keberadaan *user*. Banyak protokol gagal memenuhi kriteria *aliveness* karena jenis serangan yang sederhana. Pada banyak kasus, penyerang dapat melakukan *mirror attack* dengan mengembalikan pesan yang dikirim oleh *user* kembali kepadanya. Pada kelima protokol aplikasi ABC tidak memiliki permasalahan dalam penjaminan *aliveness*.

Walaupun tidak ada permasalahan pada kriteria *aliveness*, protokol-protokol masih memiliki kelemahan pada aspek *synchronization dan agreement*. Kriteria *aliveness* hanya berupaya untuk memastikan bahwa komunikasi yang berlangsung dilaksanakan oleh entitas asli tanpa memiliki batasan terhadap isi pesan yang dipertukarkan. Kriteria *synchronization* memiliki persyaratan autentikasi yang lebih tinggi [30]. *Synchronization* mengharuskan entitas yang berkomunikasi untuk mengirim semua pesan yang diterima dan memastikan bahwa entitas lainnya (yang sah) benar-benar menerima pesan yang dikirimkan. Artinya, komunikasi harus benar-benar berjalan sesuai dengan deskripsi protokol. Keempat protokol yang tidak lulus uji mengalami permasalahan pada kriteria *synchronization* ini [30].

Tabel 3. Rekapitulasi Temuan Kelemahan Protokol-Protokol yang Diuji

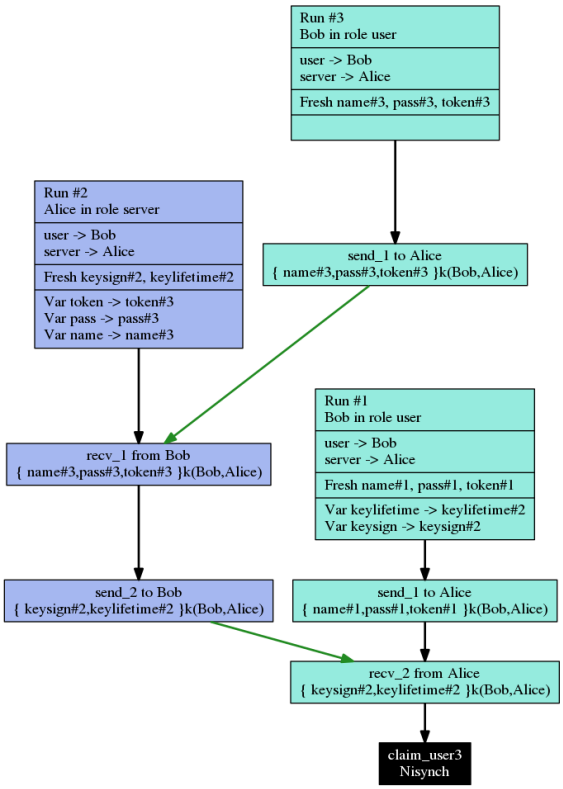
Protokol	Klaim	*Authentication*	*Secret*	Status
Registrasi	OK	*Role user*: *aliveness* *Role server*: *aliveness*	*Role user*: *email, password, authentication code* *Role server*: *verification_link, preshared_key*	**Tidak Lolos Uji**
	FAIL	*Role user*: *niagree, nisynch* *Role server*: *niagree, nisynch*	*Role user*: - *Role server*: -	
Login	OK	*Role user*: *aliveness* *Role server*: *aliveness*	*Role user*: *email, password, authentication code* *Role server*: *token*	**Tidak Lolos Uji**
	FAIL	*Role user*: *niagree, nisynch* *Role server*: *niagree, nisynch*	*Role user*: - *Role server*: -	
Pembangkitan Kunci Asimetrik	OK	*Role user*: *aliveness* *Role server*: *aliveness, niagree, nisynch*	*Role user*: *user_name, passphrase, token* *Role server*: *key_sign, key_lifetime*	**Tidak Lolos Uji**
	FAIL	*Role user*: *niagree, nisynch* *Role server*:	*Role user*: - *Role server*: -	
Permintaan Kunci Enkripsi	OK	*Role user*: *aliveness* *Role server*: *aliveness, niagree, nisynch*	*Role user*: *passphrase* *Role server*: *seedKey*	**Tidak Lolos Uji**
	FAIL	*Role user*: *niagree, nisynch* *Role server*: -	*Role user*: - *Role server*: -	
Permintaan Kunci Dekripsi	OK	*Role user*: *aliveness, niagree, nisynch* *Role server*: -	*Role user*: *seedKey* *Role server*:	**Lolos Uji**
	OK	*Role user*: - *Role server*: -	*Role user*: - *Role server*: -	

Sumber: diolah secara mandiri berdasarkan hasil pengujian

Terakhir, keempat protokol tersebut juga tidak lolos uji pada kriteria *agreement*. Kriteria *synchronization* memastikan bahwa protokol dapat berperilaku sesuai dengan deskripsi yang telah ditentukan bahkan di hadapan penyerang [30]. Kriteria *agreement* adalah kriteria autentikasi lain yang berfokus pada kesepakatan tentang pertukaran antar entitas [30]. Gagasan di balik kriteria *agreement* adalah bahwa setelah menjalankan protokol, para pihak menyepakati nilai variabel tertentu. Perjanjian tersebut didefinisikan sebagai kriteria yang mensyaratkan bahwa isi pesan mengikuti pesan yang dikirim sebagaimana ditentukan oleh protokol. Akibatnya, setelah protokol dijalankan, isi variabel akan persis seperti yang ditentukan oleh protokol [30]. Dalam konteks ini, tidak ada kemungkinan

untuk mengubah isi pesan. Jika pun terjadi perubahan, maka perubahan tersebut dapat terdeteksi. Di bawah keempat protokol Aplikasi ABC yang dinyatakan tidak lolos uji, tidak memiliki jaminan atas kriteria *synchronization* dan *agreement*.

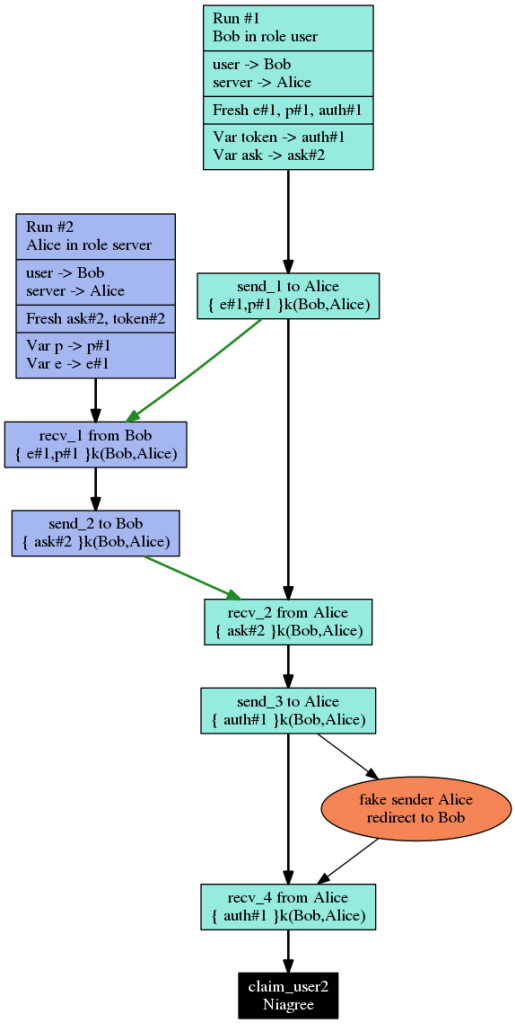
Alasan di balik tidak lulus ujinya protokol registrasi, verifikasi pengguna, pembangkitan kunci asimetrik, dan permintaan kunci enkripsi Aplikasi ABC pada kriteria *synchronization* dan *agreement* adalah karena paling tidak terdapat satu jenis serangan yang mungkin terjadi terhadap protokol-protokol tersebut yang menghilangkan jaminan *synchronization* dan *agreement*.



Gambar 14. Serangan Pada Protokol Pertukaran Kunci yang Meniadakan Jaminan Kriteria *Synchronization*
Sumber: hasil pengujian pada *Scyther*

Sebagai contoh, Serangan Pada Protokol Pertukaran Kunci yang meniadakan kriteria *synchronization*. Di mana protokol tidak dapat menjamin bahwa pihak-pihak yang terlibat dalam komunikasi adalah benar pihak-pihak yang sah berdasarkan desain. Serangan sebagaimana dimaksud diilustrasikan pada Gambar 14.

Contoh serangan lainnya adalah pada protokol verifikasi pengguna, kriteria agreement tidak terjamin akibat adanya kemungkinan pemalsuan *payload* seperti yang diilustraikan pada Gambar 15. Jenis serangan serupa juga mungkin dialami pada protokol registrasi, pembangkitan kunci asimetrik, dan permintaan kunci enkripsi.



Gambar 15. Serangan Pada Protokol Verifikasi Pengguna yang Meniadakan Jaminan Kriteria *Agreement*
Sumber: hasil pengujian pada *Scyther*

4. DISKUSI

4.1. Dampak Kelemahan Protokol

Pemodelan protokol-protokol Aplikasi ABC dilakukan dengan menyusun protokol mengikuti ketentuan *Scyther Tool*. Pada setiap protokol terdapat dua entitas, yaitu pengguna dan *server*, di mana pada pengguna selalu bertindak sebagai inisiator.

Berdasarkan temuan penelitian sebagaimana telah digambarkan pada bagian sebelumnya, masih terdapat kelemahan pada protokol-protokol yang diuji dalam aspek autentikasi, khususnya pada kriteria *sychronization* dan *agreement* untuk menjamin adanya kirim terima konten pesan yang benar dengan pihak yang benar pula.

Tingkat implementasi Aplikasi ABC yang berskala nasional menjadikan aplikasi ABC sebagai aplikasi strategis yang mana kekurangan terhadap aplikasi tersebut tidak dapat diabaikan. Adapun beberapa bahaya yang akan terjadi jika kekurangan protokol tidak ditutupi adalah:

1. Rentan terhadap eksploitasi dan yang dapat menyebabkan tidak efektifnya implementasi kebijakan.
2. Tidak sesuai dengan skema *Common Criteria* untuk produk-produk keamanan teknologi informasi.

Tidak adanya jaminan keamanan secara penuh membuka celah eksploitasi yang sering kali dapat menyebabkan permasalahan yang lebih serius di masa yang akan datang [12], [13], dan [15]. Sebagai contoh, implementasi teknologi yang ternyata memiliki celah di skala nasional akan berpotensi mengurangi kepercayaan masyarakat. Apabila kondisi terjadi, alih-alih akan menjalankan imbauan keamanan dengan menggunakan teknologi enkripsi, masyarakat akan cenderung lebih mengedepankan kepraktisan komunikasi tanpa tambahan skema enkripsi dalam melakukan tukar menukar infrormasi [39]. Kemudian, masalah ini akan diperparah bergantung pada seberapa sensitif informasi yang terlibat di dalam komunikasi tersebut. Contoh informasi strategis yang perlu dijaga keamanannya adalah informasi yang termasuk dalam informasi yang dikecualikan berdasarkan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

Selain itu, hasil pengujian menggunakan metode verifikasi formal menunjukkan bahwa protokol-protokol tersebut masih memiliki kelemahan dari sisi desain. Berdasarkan Peraturan Badan Siber dan Sandi Negara nomor 15 Tahun 2009, diatur tentang penyelenggaraan skema *Common criteria* Indonesia untuk produk-produk keamanan teknologi informasi [38]. *Common criteria* sendiri adalah sebuah kerangka kerja di mana pengguna sistem komputer dapat menentukan persyaratan fungsional dan jaminan keamanan mereka. Penyedia sistem kemudian dapat mengimplementasikan atau membuat klaim tentang atribut keamanan dari produk-produk yang mereka tawarkan. Dengan kata lain, *Common criteria* memberikan jaminan bahwa proses spesifikasi, implementasi dan evaluasi produk keamanan komputer telah dilakukan dengan cara yang ketat dan standar dan berulang pada tingkat yang sepadan dengan lingkungan target untuk digunakan [38].

Sebagai sebuah aplikasi strategis yang akan memiliki skala implementasi tingkat nasional, Aplikasi ABC harus memenuhi kriteria keamanan yang ketat. Temuan penelitian ini menandakan bahwa masih diperlukan tahap penyempurnaan sebelum Aplikasi ABC siap digunakan dalam skala besar..

4.2. Rekomendasi

Kelemahan-kelemahan yang ada pada aspek autentikasi ini dapat diselesaikan dengan bermacam-macam pendekatan. Pendekatan yang paling praktis adalah dengan menggunakan suatu penanda unik yang acak pada setiap pesan yang dikomunikasikan dalam seluruh lini komunikasi protokol. Penanda unik ini dapat berupa rangkaian bilangan yang dibangkitkan secara acak dan digunakan hanya sekali. Penanda ini disebut dengan *Cryptographic Nonce* (*number only used once*). *Cryptographic nonce* hanya dapat digunakan 1 kali untuk satu keperluan, jika terdapat *n* jumlah komunikasi, maka perlu dibankitkan *n* jumlah *cryptographic nonce*. Melalui penggunaan nonce ini, maka kriteria autentikasi *synchronization* dan *agreement* dapat dipenuhi [25] – [27]..

5. KESIMPULAN

Berdasarkan hasil pengujian, Aplikasi ABC masih memerlukan serangkaian penyempurnaan sebelum akhirnya siap digunakan pada skala besar di level nasional. Argumentasi ini sangat beralasan karena didukung oleh temuan-temuan penelitian. Hasil temuan membuktikan bahwa dari lima protokol komunikasi yang diimpelementasikan oleh Aplikasi ABC, empat protokol belum dapat memberikan jaminan aspek autentikasi khususnya pada kriteria *synchronization* dan *agreement* atas kebenaran pihak-pihak yang terlibat dalam komunikasi dan kesepakatan terhadap pesan-pesan yang dipertukarkan dalam komunikasi. Temuan penelitian ini menandakan kondisi yang bersifat kontra produktif atas setidaknya dua hal, yaitu sisi teknis desain sistem yang belum matang, dan belum adanya kepatuhan terhadap regulasi. Menimbang hasil penelitian ini sebagai kajian keamanan salah satu aplikasi pendukung komunikasi rahasia di Indonesia, Instansi XYZ perlu mengambil langkah-langkah penyesuaian sebelum akhirnya mengimplementasikan Aplikasi ABC pada skala yang lebih besar.

6. PENELITIAN BERIKUTNYA

Kelemahan-kelemahan yang teridentifikasi telah dideskripsikan dengan jelas. Untuk meningkatkan objektivitas atas hasil penelitian, pada masa yang akan datang perlu dilakukan penelitian serupa untuk objek yang sama menggunakan variasi metode verifikasi yang berbeda. Selain itu, menggunakan teori dan teknik-teknik kriptografi yang sudah ada, ke depannya perlu dipikirkan bagaimana penyesuaian-penyesuaian desain perlu dilakukan agar kelemahan-kelemahan yang ada pada protokol Aplikasi ABC dapat ditutupi.

DAFTAR PUSTAKA

[1] Ş. Eroğlu and T. Çakmak, "Information as an organizational asset: assessment of a public organization’s capabilities in Turkey," *SAGE Journals of Information Development*, vol. 36, no. 1, pp. 58-77, 2020.

[2] C. C. Aktan and İ. Y. Vural, "Bilgi C¸ agˇ ında Bilginin Yo¨netimi (Manajemen Informasi dan Jaringan Informasi)," in Bilgi

Yo¨netimi ve Bilgi Sistemleri (Manajemen Informasi dan Sistem Informasi), Konya, Çizgi Kitabevi, 2005, pp. 1-30.

[3] Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

[4] F. Cooren, T. Khun, J. P. Cornelissen and T. Clark, "Communication, Organizing and organization: An Overview and Introduction to the Special Issue," *Journals of Organization Studies (SAGE Journals Access)*, vol. 32, no. 9, pp. 1149-1170, 2011.

[5] Lee, R. R., McDonagh, J. E., Farre, A., Peters, S., Cordingley, L., & Rapley, T. "Data protection, information governance and the potential erosion of ethnographic methods in health care?" *Sociology of Health & Illness*, 44: 211– 217, 2022.

[6] BBCIndonesia, "BIN: Australia menyadap Indonesia sejak 2007," BBC Indonesia, 20 November 2013. [Online]. Available: https://www.bbc.com/indonesia/berita_indonesia/2013/11/131120_bin_sadap_australia. [Diakses pada 1 Desember 2022].

[7] BIN, "Kepala BIN: Evaluasi Sistem Keamanan Komunikasi," Badan Intelijen Negara, 28 November 2013. [Online]. Available: http://www.bin.go.id/nasional/detil/255/1/29/11/20%2013/kepala-bin-evaluasi-sistem-keamanankomunikasi. [Diakses pada 1 Desember 2020].

[8] Tempo.co, "4 Kasus Penyadapan Besar di Indonesia," Tempo, 21 February 2014. [Online]. Available: https://nasional.tempo.co/read/556304/4-kasus-penyadapan-besar-di-indonesia. [Diakses pada 1 Desember 2022].

[9] Policies For The Protection Of Critical Information Infrastructure: Ten Years Later. (2019). (). Paris: Organisation for Economic Cooperation and Development (OECD). Retrieved from ProQuest One Business; SciTech Premium Collection Retrieved from https://www.proquest.com/reports/policies-protection-critical-information/docview/2187380843/se-2.

[10] Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital.

[11] Peraturan Instansi XYZ Nomor a Tahun x Tentang Perubahan atas Peraturan Instansi XYZ Nomor b Tahun x tentang Penyelenggaraan Penilaian Kesiapan Penerapan SNI ISO/IEC 27001 Menggunakan Indeks Keamanan Informasi.

[12] M. Soriano, Information and Network Security 1st Edition, R. Gustau and S. Silvestre, Eds., Prague: Czech Technical University.

[13] J. K. Shim, A. A. Qureshi and J. G. Siegel, The International Handbook of Computer Security, United States: The Glenlake Publishing Company, Ltd, 2000.

[14] A. J. Menezes, S. A. Vanstone and P. C. Van Oorschot, Handbook of Applied Cryptography, United States: CRC Press, 1997.

[15] J. Andres, "The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice," Syngress Media Incorporated, Amsterdam, 2011.

[16] Instansi XYZ, Dokumentasi Aplikasi ABC, 2021 (*unpublished*)

[17] S. S. Emami, Security Analysis of Cryptographic Algorithms, Sydney: Macquarie University, 2013.

[18] Q. Chen, C. Zhang and S. Zhang, "Overview of Security Protocol Analysis," in *Secure Transaction Protocol Analysis, Lecture Notes in Computer Science*, Vol 5111, Heidelberg, Springer, 2008.

[19] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

[20] N. Z. Almuzaini and I. Ahmad, "Formal Analysis of the Signal Protocol Using the Scyther Tool," 2019 2nd *International Conference on Computer Applications & Information Security (ICCAIS)*, pp. 1-6, 2019, doi: 10.1109/CAIS.2019.8769532.

[21] Fikri, M. A., Ramli, K., & Sudiana, D., "Formal verification of the authentication and voice communication protocol security on device X using scyther tool," *IOP Conference Series. Materials Science and Engineering*, 1077(1), 2019, doi:https://doi.org/10.1088/1757-899X/1077/1/012057.

[22] Shaik Shakeel Ahamad & Al-Sakib Khan Pathan, "A formally verified authentication protocol in secure framework for mobile healthcare during COVID-19-like pandemic," Connection Science, 33:3, 532-554, 2021, doi: 10.1080/09540091.2020.1854180

[23] N. E., Madhoun, F. Guenane, G. Pujolle, "An online security protocol for NFC payment: Formally analyzed by the scyther tool," *Second International Conference on Mobile and Secure Services (MobiSecServ)*, pp. 1-7, 2016, doi: 10.1109/MOBISECSERV.2016.7440225.

[24] P. R. Babu, A. G. Reddy, B. Palaniswamy and S. K. Kommuri, "EV-Auth: Lightweight Authentication Protocol Suite for Dynamic Charging System of Electric Vehicles With

Seamless Handover," in *IEEE Transactions on Intelligent Vehicles*, vol. 7, no. 3, pp. 734-747, Sept. 2022, doi: 10.1109/TIV.2022.3153658.

[25] S. Rostampour, M. Safkhani, et al. "ECCbAP: A secure ECC-based authentication protocol for IoT edge devices," *Pervasive and Mobile Computing*, Volume 67, ISSN 1574-1192, 2020 doi: https://doi.org/10.1016/j.pmcj.2020.101194.

[26] H. Huang, S. Lu, Z. Wu, et al, "An efficient authentication and key agreement protocol for IoT-enabled devices in distributed cloud computing architecture," *J Wireless Com Network*, 150, 2021, https://doi.org/10.1186/s13638-021-02022-1.

[27] M. Hosseinzadeh et al., "A New Strong Adversary Model for RFID Authentication Protocols," in *IEEE Access*, vol. 8, pp. 125029-125045, 2020, doi: 10.1109/ACCESS.2020.3007771.

[28] M. Avalle, A. Pironti and R. Sisto, "Formal Verification of Security Protocol Implementations: a Survey," *Form Asp Comp*, vol. 26, pp. 99-123, 2014.

[29] R. Chadha, V. Cheval, Ş. Ciobâcă and S. Kremer, "Automated Verification of Equivalence Properties of Cryptographic Protocols," *ACM Transactions on Computational Logic*, vol. 17, no. 4, p. Article 23, 2016.

[30] Cremers, C., Mauw, S., Operational Semantics and Verification of Security Protocols, ISSN 1619-7100, Springer Berlin, Heidelberg, 2012, doi: https://doi.org/10.1007/978-3-540-78636-8.

[31] El Madhoun, N., Bertin, E., Badra, M. et al. (2021). Towards more secure EMV purchase transactions. Ann. Telecommun. 76, 203–222, doi: https://remote-lib.ui.ac.id:2075/10.1007/s12243-020-00784-1

[32] R. Amin, S. Kunal et al, "CFSec: Password based secure communication protocol in cloud-fog environment," *Journal of Parallel and Distributed Computing*, Volume 140, Pages 52-62, ISSN 0743-7315, 2020, doi: https://doi.org/10.1016/j.jpdc.2020.02.005.

[33] A.K. Yadav, M. Misra, et al, "An improved and provably secure symmetric-key based 5G-AKA Protocol," *Computer Networks*, Volume 218, ISSN 1389-1286, 2022, doi: https://doi.org/10.1016/j.comnet.2022.109400.

[34] M. Farokhlagha, S. Masoumeh, "SEOTP: A new secure and efficient ownership transfer protocol based on quadric residue and homomorphic encryption," *Wireless Networks*, 26(7), 5285-5306, 2022, doi:https://doi.org/10.1007/s11276-020-02397-x.

[35] M. Bouchaala, C. Ghazel, L.A. Saidane, "Enhancing security and efficiency in cloud computing authentication and key agreement scheme based on smart card," *J Supercomput 78*, 497–522, 2022, doi:https://remote-lib.ui.ac.id:2075/10.1007/s11227-021-03857-7.

[36] F.G. Darbandeh, M. Safkhani, "A New Lightweight User Authentication and Key Agreement Scheme for WSN," *Wireless Pers Commun 114*, 3247–3269, 2020, doi: https://remote-lib.ui.ac.id:2075/10.1007/s11277-020-07527-4.

[37] Ahamad S. S., "A Novel NFC-Based Secure Protocol for Merchant Transactions," *IEEE Access*, vol. 10, pp. 1905-1920, 2022, doi: 10.1109/ACCESS.2021.3139065.

[38] Peraturan Badan Siber dan Sandi Negara nomor 15 Tahun 2009, diatur tentang penyelenggaraan skema Common criteria Indonesia.

[39] Hsiao, R., "Technology fears: Distrust and cultural persistence in electronic marketplace adoption," *The Journal of Strategic Information Systems*. 12. 169-199, 2003, doi:10.1016/S0963-8687(03)00034-9..