

# Analisis dan Verifikasi Protokol Kriptografi Aplikasi Manajemen Kunci Menggunakan Scyther: Studi Kasus Aplikasi XYZ

Indra Dimas Nurdiyanto\*<sup>1</sup>, Ruki Harwahyu<sup>2</sup>

<sup>1,2</sup>Departement Teknik Elektro, Universitas Indonesia

E-mail: \*[indra.dimas@ui.ac.id](mailto:indra.dimas@ui.ac.id)

## Abstrak

*Abstrak— Semakin meningkatnya ancaman dan serangan yang mengakibatkan kebocoran data di Indonesia sejalan dengan pesatnya perkembangan teknologi dan informasi. Menjawab tantangan tersebut instansi ABC mengembangkan aplikasi XYZ sebagai salah satu solusi dalam pengamanan data dan informasi. Oleh karena itu, untuk memastikan kemampuan aplikasi tersebut dalam memberikan jaminan keamanan kepada pengguna, pada penelitian ini dilakukan analisis dan verifikasi keamanan protokol kriptografi aplikasi XYZ. Analisis dan verifikasi dilakukan melalui pendekatan verifikasi formal menggunakan alat bantu Scyther dengan focus pada protokol verifikasi pengguna, pembangkitan kunci, dan permintaan kunci untuk proses enkripsi-dekripsi. Hasil analisis menunjukkan bahwa protokol-protokol tersebut telah memenuhi kriteria secrecy untuk informasi rahasia yang ditransmisikan namun memiliki kelemahan pada aspek autentikasi. Penerapan sharedsecret dan rangkaian cryptographic nonce terbukti mampu mengatasi kelemahan pada protokol verifikasi pengguna aplikasi XYZ.*

**Kata Kunci—** Aplikasi XYZ, Protokol Kriptografi, Scyther Tool

## 1. PENDAHULUAN

Saat ini sistem informasi dan informasi yang dikandungnya merupakan aset penting bagi setiap organisasi yang memerlukan perlindungan[1]. Informasi yang digunakan oleh pemerintah dan bisnis tersimpan dalam suatu sistem baik secara stand alone (tanpa terkoneksi jaringan) maupun dalam jaringan komputer yang saling terhubung, misalnya internet. Karena Internet dibagi oleh organisasi dan individu yang beragam dan tentunya terdapat persaingan didalamnya, sehingga sistem informasi harus terlindung dari adanya ancaman pengungkapan, modifikasi, dan penggunaan yang tidak sah [1].

Penggunaan mekanisme kriptografi adalah salah satu cara terkuat untuk menyediakan layanan keamanan untuk aplikasi dan protokol elektronik dan untuk penyimpanan data [2]. Sebagai upaya untuk memberikan perlindungan dan menjamin kerahasiaan informasi melalui penerapan mekanisme kriptografi, instansi ABC telah mengeluarkan aplikasi pengamanan data (aplikasi XYZ). Aplikasi XYZ digunakan untuk kebutuhan pengelolaan kunci kriptografi dan pengamanan data dan informasi. Keamanan informasi dalam proses tersebut berfokus pada kerahasiaan, keutuhan dan ketersediaan informasi [3]-[5]. Aplikasi XYZ telah digunakan mulai tahun 2022 pada beberapa instansi di bidang administrasi pemerintahan. Untuk memberikan jaminan kehandalan aplikasi XYZ maka perlu dilakukan analisis keamanan protokol kriptografi terhadap aplikasi tersebut. Untuk melakukan analisis protokol kriptografi umumnya dilakukan melalui dua pendekatan yaitu verifikasi formal dan pengamatan langsung, baik dengan menggunakan alat bantu, maupun tidak [6], [7]. Salah satu alat bantu verifikasi formal protokol kriptografi yang populer adalah Scyther Tool [8]. Dalam beberapa tahun terakhir alat bantu Scyther telah banyak digunakan untuk melakukan pengujian terhadap aspek autentikasi dan kerahasiaan pada protokol -protokol baru [9]-[15].

Oleh karena itu, melalui pendekatan formal dengan alat bantu Scyther, penulis melakukan analisis keamanan protokol kriptografi yang berjalan pada aplikasi manajemen kunci XYZ sebagai salah satu aplikasi yang digunakan dalam pengelolaan kunci kriptografi.

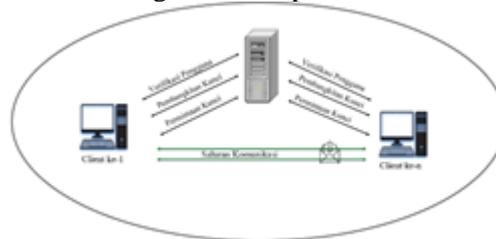
### 1.1. Studi Literatur

Pada bagian ini dijelaskan tentang Aplikasi XYZ, Manajemen Kunci Kriptografi, dan Scyther tool.

#### 1.1.1. Aplikasi XYZ

Aplikasi XYZ merupakan aplikasi yang menyediakan layanan pengelolaan kunci kriptografi. Aplikasi ini dapat digunakan pada perangkat Personal Computer (PC) atau laptop dengan sistem operasi Windows, Mac OS dan Linux. Aplikasi XYZ dibangun di atas arsitektur client-server. Server yang digunakan berfungsi sebagai pengelolaan pengguna dan manajemen kunci terpusat. Seluruh perangkat yang terkoneksi menggunakan Aplikasi XYZ berkomunikasi dengan server ini untuk menyelesaikan tahapan verifikasi pengguna, pembangkitan kunci dan permintaan kunci untuk melakukan enkripsi.

Adapun arsitektur Aplikasi XYZ digambarkan pada Gambar 2.1.



Gambar 1 Arsitektur Sistem Aplikasi XYZ

Pada aplikasi XYZ terdapat tiga aplikasi yang berjalan, yaitu:

1. Protokol Verifikasi Pengguna Aplikasi XYZ
2. Protokol pembangkitan kunci
3. Protokol permintaan kunci untuk proses enkripsi dan dekripsi

#### 1.1.2. Manajemen Kunci Kriptografi

Manajemen kunci memainkan peranan penting dalam kriptografi sebagai dasar untuk melakukan pengamanan teknik kriptografi yang menyediakan kerahasiaan, autentikasi entitas, autentikasi sumber data, integritas data, dan tanda tangan digital [16]. Berdasarkan [17] manajemen kunci merupakan aktivitas yang menyertakan pemeliharaan kunci kriptografi dan parameter keamanan lainnya (misal initialization vectors) dalam seluruh siklus hidup kunci yang mencakup pembangkitan, penyimpanan, penetapan, masuk dan keluar, serta penghancuran kunci.

Manajemen kunci kriptografi yang tepat sangat penting untuk penggunaan kriptografi yang efektif untuk keamanan. Keamanan informasi yang dilindungi oleh kriptografi secara langsung bergantung pada kekuatan kunci, keefektifan mekanisme dan protokol yang terkait dengan kunci, dan perlindungan yang diberikan pada kunci. Semua kunci perlu dilindungi dari modifikasi, dan dari pengungkapan yang tidak sah.

### 1.1.3. Scyther Tool

Scyther Tool merupakan hasil penelitian Cas Cremers pada tahun 2006. Pada saat itu, Cas Cremers mempublikasikan penelitiannya terkait metodologi analisis formal dan verifikasi protokol kriptografi berupa alat analisis yang dikenal dengan nama Scyther Tool. Alat ini dapat menganalisis sifat kerahasiaan (secrecy) dan autentikasi dalam suatu protokol kriptografi. Dengan Alat Scyther, objektivitas verifikasi protokol formal dapat dijamin.

Dalam scyther tool terdapat dua klaim untuk memodelkan properti keamanan secrecy (kerahasiaan) dan Autentikasi.

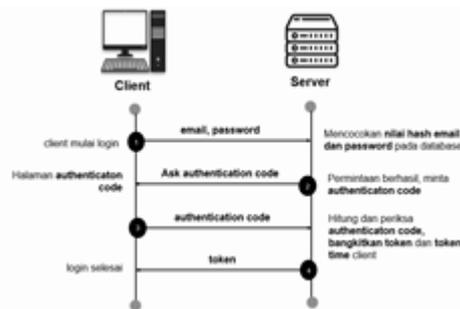
1. Secrecy. Klaim Kerahasiaan yang menyatakan bahwa informasi tertentu tidak diungkapkan kepada pihak yang tidak berhak meskipun data tersebut dikomunikasikan melalui jaringan yang tidak dipercaya.
2. Autentikasi. Autentikasi ada untuk memastikan keberadaan pihak yang berkomunikasi. Ada tiga kriteria autentikasi, yaitu aliveness, synchronization, and agreement.
  - a. Aliveness: bentuk autentikasi yang bertujuan untuk memastikan bahwa pihak yang berkomunikasi telah melakukan beberapa peristiwa, yang menunjukkan bahwa pihak tersebut 'Alive'.
  - b. Synchronization: untuk memastikan bahwa pesan telah dikirim atau diterima oleh pihak yang berkomunikasi. Synchronization hanya meninjau konten dan menyortir pesan.
  - c. Agreement: bentuk autentikasi yang berfokus kesepakatan data yang dipertukarkan antar pihak, yang mengharuskan isi pesan yang diterima cocok dengan pesan yang dikirim sebagaimana ditentukan oleh protokol.

## 2. METODE PENELITIAN

Terdapat tiga protokol yang menjadi objek penelitian yaitu protokol verifikasi pengguna, pembangkitan kunci, dan permintaan kunci untuk proses enkripsi dan dekripsi.

### 2.1. Pemodelan

#### 2.1.1. Protokol Verifikasi Pengguna



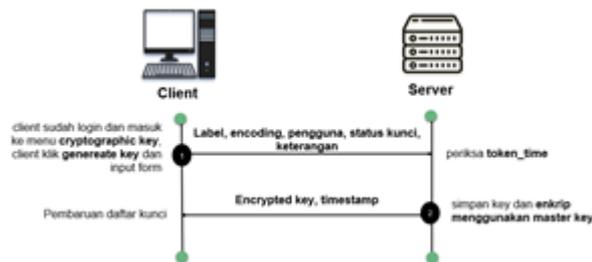
Gambar 2 Protokol Verifikasi Pengguna

Proses verifikasi berjalan pada saat client melakukan login untuk masuk ke dalam aplikasi. Client akan memasukkan email dan password pada form login. Setelah client mengisi form, maka email dan password tersebut akan dikirimkan ke server untuk dilakukan pencocokan

nilai hash dari email dan password yang tersimpan di dalam database. Apabila nilai hash tersebut cocok, maka server akan mengirimkan kode autentikasi untuk dikirimkan melalui TOTP.

Setelah client 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 client tersebut benar, maka server akan membangkitkan token dan token\_time untuk client dapat masuk kedalam sesi aplikasi. Setelah token dan token\_time dikirimkan oleh server kepada client, maka client dapat mengakses fitur aplikasi dengan jangka waktu sesuai dengan pengaturan waktu sesi yang ada di dalam token\_time.

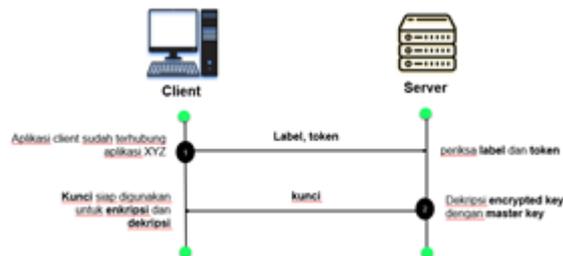
2.1.2. Pembangkitan Kunci



Gambar 3 Protokol Pembangkitan Kunci

Kunci yang dibangkitkan adalah kunci simetris yang akan digunakan oleh client untuk pengamanan data dan informasi dalam proses komunikasi. Dalam proses pembangkitan kunci digunakan beberapa parameter khusus. Setelah kunci tersebut dibangkitkan, selanjutnya kunci disimpan di dalam database milik server dalam bentuk terenkripsi menggunakan Master Key server.

2.1.3. Permintaan Kunci Untuk Proses Enkripsi dan dekripsi



Gambar 4 Protokol Permintaan Kunci Untuk Proses Enkripsi dan dekripsi

Client akan mengirimkan permintaan kunci kepada server. Server akan melakukan validasi pada Label Kunci dan Token untuk mengecek apakah Label Kunci dan Token yang dikirimkan terdapat di database atau tidak. Apabila cocok maka server akan melakukan dekripsi kunci menggunakan Master Key server. Kemudian kunci yang telah didekripsi dikirimkan kepada client untuk dapat digunakan dalam proses enkripsi dan dekripsi file

2.2. Pengujian

Seperti disebutkan pada bagian sebelumnya, protokol aplikasi XYZ dianalisis dalam tiga fase, protokol verifikasi pengguna, pembangkitan kunci, dan permintaan kunci untuk proses enkripsi-dekripsi. Analisis dalam penelitian ini menggunakan pendekatan model checking. Tiga fase yang disebutkan diuji terhadap persyaratan keamanan. Pengecekan model dilakukan dengan

menggunakan alat Scyther, yang merupakan alat pengecekan model. Spesifikasi fase protokol sinyal dimodelkan sebagai peristiwa klaim. Properti keamanan fase protokol aplikasi XYZ diverifikasi berdasarkan pengujian yang dilakukan.

2.2.1. Model Checking Protokol Verifikasi Pengguna

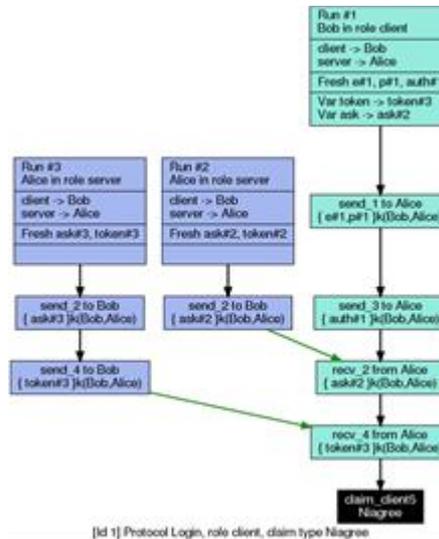
Pada Potokol verifikasi pengguna menunjukkan hasil verifikasi protokol verifikasi pengguna aplikasi XYZ pada gambar 5. Dari sepuluh claim, terdapat enam claim yang dinyatakan benar atau OK dan empat claim dinyatakan gagal atau FAIL.

Claim	Status	Comments	Pattern
Login_client	OK	Verified	No attacks.
Login_client2	OK	Verified	No attacks.
Login_client3	OK	Verified	No attacks.
Login_client4	OK	Verified	No attacks.
Login_client5	Fail	Falsified	Exactly 1 attack. 1 attack
Login_client6	Fail	Falsified	Exactly 1 attack. 1 attack
server	OK	Verified	No attacks.
Login_server2	OK	Verified	No attacks.
Login_server3	Fail	Falsified	Exactly 1 attack. 1 attack
Login_server4	Fail	Falsified	Exactly 1 attack. 1 attack

Gambar 5 Model Checking Verifikasi Protokol Verifikasi Pengguna

Tidak terpenuhinya claim disebabkan karena berdasarkan hasil pengujian, paling tidak terdapat satu jenis serangan yang mungkin terhadap protokol tersebut. Adapun penjelasan tentang grafik serangan yang mungkin pada masing-masing claim yang gagal adalah sebagai berikut.

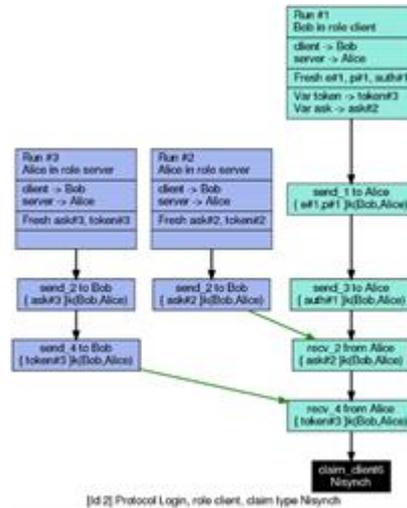
1. Serangan pada claim authentication tipe agreement oleh role client  
Klaim autentikasi dengan tipe agreement pada protokol verifikasi pengguna untuk role client tidak terpenuhi akibat terdapat kemungkinan serangan atas kondisi tersebut di dalam protokol. Serangan tersebut ditunjukkan pada Gambar 6.



Gambar 6 Serangan Klaim Agreement oleh Role Client Pada Protokol Verifikasi Pengguna

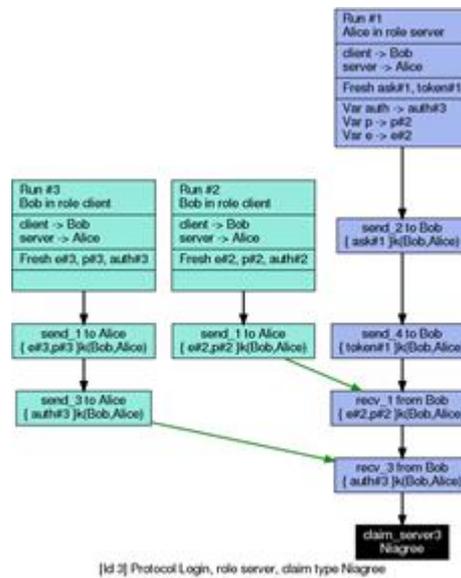
2. Serangan pada claim authentication tipe synchronization oleh role client  
Klaim autentikasi dengan tipe synchronization pada rotocol verifikasi pengguna untuk role client tidak terpenuhi akibat terdapat kemungkinan serangan

atas kondisi tersebut di dalam rotocol. Serangan tersebut ditunjukkan pada Gambar 7.



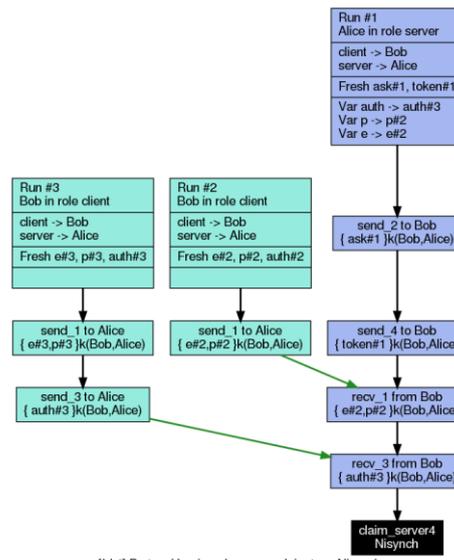
Gambar 7 Skenario Serangan Klaim Synchronization oleh Role Client Pada Protokol Verifikasi Pengguna

3. Serangan pada claim authentication tipe agreement oleh role server  
Klaim autentikasi dengan tipe agreement pada protokol verifikasi pengguna untuk role server tidak terpenuhi akibat terdapat kemungkinan serangan atas kondisi tersebut di dalam protokol. Serangan tersebut ditunjukkan pada Gambar 8.



Gambar 8 Skenario Serangan Klaim Agreement oleh Role Server Pada Protokol Verifikasi Pengguna

4. Serangan pada claim authentication tipe synchronization oleh role server  
Klaim autentikasi dengan tipe synchronization pada rotocol verifikasi pengguna untuk role server tidak terpenuhi akibat terdapat kemungkinan serangan atas kondisi tersebut di dalam rotocol. Serangan tersebut ditunjukkan pada Gambar 9.



[Id 4] Protocol Login, role server, claim type Nisynch

Gambar 9 Skenario Serangan Klaim Synchronization oleh Role Server Pada Protokol Verifikasi Pengguna

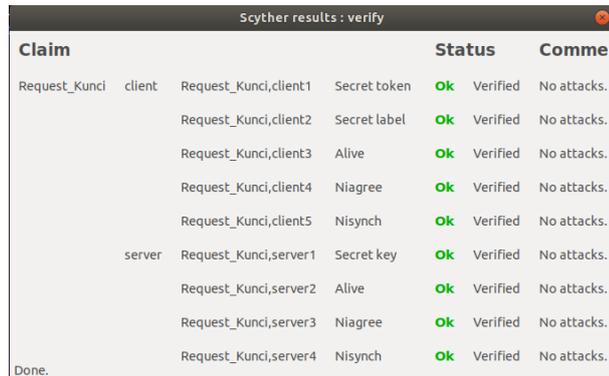
2.2.2. Model Checking Protokol Pembangkitan Kunci

Claim	Status	Commer
Generate_Kunci client Generate_Kunci_client1 Secret label	OK Verified	No attacks.
Generate_Kunci_client2 Secret encoding	OK Verified	No attacks.
Generate_Kunci_client3 Secret pengguna	OK Verified	No attacks.
Generate_Kunci_client4 Secret status	OK Verified	No attacks.
Generate_Kunci_client5 Secret token	OK Verified	No attacks.
Generate_Kunci_client6 Alive	OK Verified	No attacks.
Generate_Kunci_client7 Niagree	OK Verified	No attacks.
Generate_Kunci_client8 Nisynch	OK Verified	No attacks.
server Generate_Kunci_server1 Secret encryptedkey	OK Verified	No attacks.
Generate_Kunci_server2 Secret timestamp	OK Verified	No attacks.
Generate_Kunci_server3 Alive	OK Verified	No attacks.
Generate_Kunci_server4 Niagree	OK Verified	No attacks.
Generate_Kunci_server5 Nisynch	OK Verified	No attacks.

Gambar 10 Model Checking Verifikasi Protokol Pembangkitan Kunci

Hasil verifikasi protokol pembangkitan kunci pada Gambar 10 menunjukkan bahwa dari tiga belas claim yang diuji menunjukkan bahwa semua claim yang dinyatakan benar atau OK. Pengujian ini menunjukkan bahwa protokol ini memenuhi properti keamanan untuk aspek secrecy dan autentikasi.

### 2.2.3. Model Checking Protokol Permintaan Kunci Untuk Proses Enkripsi dan dekripsi



Claim	Status	Commer
Request_Kunci client Request_Kunci,client1 Secret token	OK Verified	No attacks.
Request_Kunci,client2 Secret label	OK Verified	No attacks.
Request_Kunci,client3 Alive	OK Verified	No attacks.
Request_Kunci,client4 Niagree	OK Verified	No attacks.
Request_Kunci,client5 Nisynch	OK Verified	No attacks.
server Request_Kunci,server1 Secret key	OK Verified	No attacks.
Request_Kunci,server2 Alive	OK Verified	No attacks.
Request_Kunci,server3 Niagree	OK Verified	No attacks.
Request_Kunci,server4 Nisynch	OK Verified	No attacks.

Gambar 11 Model Checking Verifikasi Protokol Permintaan Kunci untuk Proses Enkripsi-Dekripsi

Hasil verifikasi protokol permintaan kunci untuk proses enkripsi-dekripsi menunjukkan bahwa sembilan claim yang diuji, menyatakan bahwa semua claim dinyatakan benar atau OK. Pengujian ini menunjukkan bahwa protokol ini memenuhi properti keamanan untuk aspek secrecy dan autentikasi.

## 3. HASIL DAN PEMBAHASAN

### 3.1. Hasil dan Analisis

Dalam penelitian ini, protokol aplikasi XYZ dianalisis dengan pendekatan model checking dan asumsi perfect cryptography yaitu mengasumsikan bahwa keseluruhan fungsi kriptografi adalah perfect [8]. Kelemahan utama dari protokol aplikasi XYZ adalah adanya kerentanan dalam aspek autentikasi pada protokol verifikasi pengguna. Client dan Server mengalami kegagalan yang sama dalam pemenuhan kriteria keamanan pada claim tipe autentikasi yaitu synchronization dan agreement.

Kegagalan pertama, yaitu pada kriteria synchronization. Sebagaimana digambarkan pada Gambar 7 dan Gambar 9, pola-pola serangan tersebut membuktikan bahwa tidak terdapat jaminan bahwa pesan yang diterima client adalah benar berasal dari server dan begitu pula sebaliknya. Pada protokol verifikasi pengguna terdapat pihak yang dapat berpura-pura sebagai mitra komunikasi sehingga menghilangkan jaminan kebenaran mitra komunikasi.

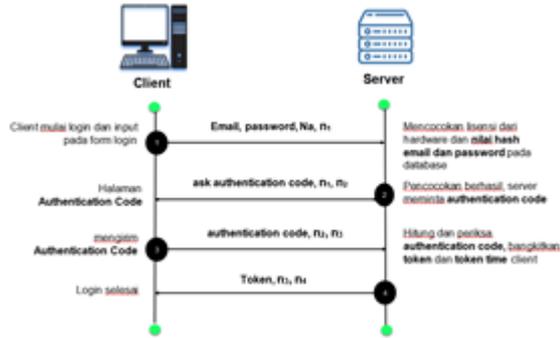
Kegagalan kedua, yaitu pada kriteria agreement. Setelah protokol verifikasi pengguna dijalankan, isi variabel seharusnya terjamin sama persis seperti yang ditentukan oleh protokol. Dalam artian tidak terdapat kemungkinan untuk merubah isi dari pesan. Jika pun terjadi, maka hal tersebut dapat diketahui oleh pihak-pihak yang terlibat. Pada protokol verifikasi pengguna, tidak terdapat jaminan akan isi pesan yang dikirim sebagaimana kemungkinan yang diilustrasikan dalam serangan pada Gambar 6 dan Gambar 8.

Pada protokol pembangkitan kunci dan permintaan kunci untuk proses enkripsi-dekripsi menunjukkan bahwa kedua protokol tersebut memenuhi properti keamanan untuk aspek secrecy dan autentikasi.

### 3.2. Rekomendasi

Untuk mengatasi adanya kerentanan pada aspek autentikasi dalam protokol kriptografi, pada penelitian ini penulis mengajukan untuk penerapan Lisensi dan Cryptographic Nonce

(number only used once). Lisensi digunakan untuk mengenali perangkat yang digunakan dalam proses operasional aplikasi. Lisensi ini berupa sharedsecret antara client dan server. Cryptographic nonce diterapkan 1 kali untuk satu keperluan, jika terdapat n jumlah komunikasi, maka perlu dibangkitkan n jumlah cryptographic nonce. Model protokol perbaikan untuk protokol verifikasi pengguna sebagai berikut:



Gambar 12 Protokol Verifikasi Pengguna Perbaikan

Hasil verifikasi protokol perbaikan yang dihasilkan dengan model checking menunjukkan bahwa klaim dari semua properti keamanan telah terpenuhi, status OK.

Claim	Status	Commer
verifikasi_login_client	OK	Verified
verifikasi_login_client2	OK	Verified
verifikasi_login_client3	OK	Verified
verifikasi_login_client4	OK	Verified
verifikasi_login_client5	OK	Verified
verifikasi_login_client6	OK	Verified
server	OK	Verified
verifikasi_login_server1	OK	Verified
verifikasi_login_server2	OK	Verified
verifikasi_login_server3	OK	Verified
verifikasi_login_server4	OK	Verified

Berdasarkan hasil pengujian, penerapan lisensi dan cryptographic nonce pada protokol verifikasi pengguna telah dibuktikan mampu memberikan penguatan pada kriteria synchronization dan agreement

Tabel 1 Perbandingan Protokol Verifikasi Pengguna sebelum dan sesudah perbaikan

No	Nama Protokol	Klaim	Protokol awal		Protokol Perbaikan	
			Security Control	Status	Security Control	Status
1	Verifikasi Pengguna	Kerahasiaan (secret)	Encryption key	OK	Encryption key	OK
		keabsahan (authentic)	Communication Channel	OK	Communication Channel	OK
		jaminan pengiriman dan penerimaan pesan (synchronization)	-	FAIL	Cryptographic Nonce	OK
		jaminan isi pesan (agreement)	-	FAIL	Cryptographic Nonce	OK

#### 4. KESIMPULAN

Protokol Aplikasi XYZ diuji dengan menggunakan Scyther pada fase verifikasi pengguna, pembangkitan kunci, dan permintaan kunci untuk proses enkripsi-dekripsi. Penggunaan tool ini berfokus pada aspek jaminan kerahasiaan informasi dan autentikasi dengan

empat kriteria yaitu secrecy, aliveness, synchronization, dan agreement. Hasil penelitian menunjukkan bahwa protokol-protokol tersebut telah memenuhi kriteria secrecy untuk informasi rahasia yang ditransmisikan namun memiliki kelemahan pada autentikasi khususnya untuk kriteria synchronization dan agreement pada protokol verifikasi pengguna. Penerapan sharedsecret dan rangkaian cryptographic nonce terbukti mampu mengatasi kelemahan pada protokol verifikasi pengguna aplikasi XYZ.

#### DAFTAR PUSTAKA

- [1] Barker. Elain, Miles Smid and Dennis Branstad. NIST Special Publication 800-152. A Profile for U.S. Federal Cryptographic Key Management Systems. National Institute of Standards and Technology. 2015.
- [2] Barker. Elain. NIST Special Publication 800-57 Revision 5. Recommendation for Key Management Part-1 : General. National Institute of Standards and Technology. 2020.
- [3] M. Soriano, Information and Network Security 1st Edition, R. Gustau and S. Silvestre, Eds., Prague: Czech Technical University.
- [4] J. K. Shim, A. A. Qureshi and J. G. Siegel, The International Handbook of Computer Security, United States: The Glenlake Publishing Company, Ltd, 2000.
- [5] A. J. Menezes, S. A. Vanstone and P. C. Van Oorschot, Handbook of Applied Cryptography, United States: CRC Press, 1997.
- [6] M. Avalle, A. Pironti and R. Sisto, "Formal Verification of Security Protocol Implementations: a Survey," Form Asp Comp, vol. 26, pp. 99-123, 2014.
- [7] R. Chadha, V. Cheval, Ş. Ciobăcă and S. Kremer, "Automated Verification of Equivalence Properties of Cryptographic Protocols," ACM Transactions on Computational Logic, vol. 17, no. 4, p. Article 23, 2016.
- [8] 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>.
- [9] 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>
- [10] 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>.
- [11] 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>.
- [12] 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>.
- [13] 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>.
- [14] 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>.

- [15] 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.
- [16] A. J. Menezes, S. A. Vanstone and P. C. Van Oorschot, Handbook of Applied Cryptography, United States: CRC Press, 1997.
- [17] Barker, Elaine, William Barker, William Burr, William Polk, & Miles Smid. Recommendation for Key Management – Part 1: General (Revision 4), NIST Special Publication 800-57, US Department of Commerce. 2016.