OPEN ACCESS
J. OF INISTA, VOL. 2, NO. 2, PP.054-060, MAY 2020

ISSN : 2622-8106 (ONLINE)
DOI: 10.20895/INISTA.V2I2

Journal of Informatics, Information System, Software Engineering and Applications

Desain *Digital Right Management* (DRM) Untuk Perangkat Lunak Berbasis *Desktop* Menggunakan Teknik *Mutual Authentication*

Yoso Adi Setyoko

Fakultas Informatika, Institut Teknologi Telkom Purwokerto
Jalan D.I. Pandjaitan No. 128 Purwokerto

yoso@ittelkom-pwt.ac.id,

Accepted on 19-05-2020

Abstrak

Software yang tergolong sebagai aplikasi desktop cukup rentan dari bentuk pembajakan. Pembajakan perangkat lunak di Indonesia untuk Microsoft Office terdapat 177480 salinan perangkat lunak. Selain itu Indonesia saat ini masih menduduki peringkat kedua pembajakan software di Asia Pasifik dengan skor 83 persen. Pembajakan terhadap *software* sangat mudah yaitu dengan cara menduplikat software tersebut. Untuk menanggulangi permasalahan duplikasi aplikasi tersbut maka dibutuhkan mekanisme perlindungan data yang disebut sebagai *Digital Right Management* (DRM). Beberapa pihak pembuat software telah menerapkan teknik-teknik DRM contohnya dengan menggunakan *Public Key Infrasturktur* (PKI), kemudian dengan teknik penggunaan kode lisensi, serta Attribute Based Access Control (ABAC).Sedangkan penelitian kami saat ini melakukan pendekatan lain dalam pembuatan DRM yaitu menggunakan teknik rekayasa protokol jaringan yang disebut dengan proses *Mutual Authenticataion* atau autentikasi dua arah. Pada tahun 2004 Philips menerbitkan sebuah dokumen dan protokol yang digunakan untuk komunikasi *smart card* dan *reader*-nya. Protokol yang dibuat oleh Philips di dalamnya menggunakan teknik *Mutual Authentication*. Mutual Authentication merupkan langkah untuk melakukan autentikasi dua belah pihak proses inisialisasi komunikasi. Pada penelitian ini penulis mengadopsi protokol tersebut untuk diterapkan sebagai DRM. Hasil penelitian kami dapat membuktikan secara sistematis bahwa protokol hasil adopsi dan modifikasi tersebut mampu mengamankan komunikasi yang dilakukan antara *client (software)* dan *server* menggunakan analisis ancaman dan upaya pengamanan protokol. Celah yang dapat ditanggulangi melalui protokol ini adalah celah kebocoran kunci, celah kebocoran autentikasi, dan celah kebocoran pertukaran data.

Keywords: DRM, *key diversification*, *mutual authentication*, *secure channel*, protokol, *Philips Semiconductor*.

I. PENDAHULUAN

Saat ini perangkat lunak yang berbasis *desktop* yang di-*install* langsung di komputer masih digunakan oleh beberapa badan usaha. Salah satu keunggulan perangkat lunak *desktop* adalah tidak memerlukan koneksi internet. Perangkat lunak berbasis desktop saat ini umumnya menggunakan verifikasi *serial number* yang dilakukan sekali menggunakan koneksi internet. Contoh aplikasi-aplikasi tersebut adalah Microsoft Office, AutoCad, Photoshop, Corel Draw yang saat ini masih sangat banyak digunakan oleh personal maupun badan usaha. Namun, keberadaanya saat ini luput terhadap perlindungan data. Banyak perangkat lunak yang dibajak berhasil dibajak oleh pengguna aplikasi itu sendiri. Menurut informasi yang diperoleh dari kabar24.bisnis.com menyatakan bahwa di Indonesia pada tahun 2006 terdapat 177480 salinan perangkat lunak Microsoft Office.

Kemudian di tahun 2020 Indonesia menduduki peringkat kedua pembajakan software di Asia Pasifik sebesar 83 persen [8]. Oleh karena itu, suatu perangkat lunak membutuhkan perlindungan terhadap pembajakan. Perlindungan terhadap pembajakan tersebut dinamakan dengan *Digital Right Management* (DRM). Menurut penelitian [3] DRM dibagi menjadi 4 pilar yaitu *encryption, conditional access, copy policy, identification and tracking*. Pilar *encryption* mencakup teknik mengenkripsi konten digital, *conditional access* adalah pembuatan kontrol akses ke perangkat lunak, *copy policy* mencakup pengaturan terhadap pengubahan dan duplikasi data, sedangkan *identification and tracking* mencakup kontrol penyebaran penggunaan data digital.

Beberapa penelitian terkait mengenai DRM adalah pemakaian *Public Key Infrastructure* (PKI) untuk mekanisme autentikasi pengguna dengan pemilik perangkat lunak [1]. Penelitian ini melakukan perlindungan terhadap perangkat lunak secara *online*. Yang dilakukan oleh penelitian [1] adalah autentikasi antara perangkat lunak dengan server PKI secara online. Kemudian untuk penelitian kedua juga merancang teknik autentikasi antara perangkat lunak yang dilakukan secara *online*. Penelitian kedua melakukan dua kali proses autentikasi *online* yaitu antara *client* dengan *server* autentikasi serta antara *client* dengan *server* lisensi pada *channel* televisi [2]. Penelitian selanjutnya yaitu penelitian [3] melakukan proses DRM dengan memanfaatkan *access control* yaitu dengan teknik *Attribute Based Access Control* (ABAC). ABAC adalah bagian dari teknik DRM yang melakukan identifikasi pengguna perangkat lunak menggunakan atribut yang dimiliki oleh pengguna maupun atribut yang dimiliki oleh perangkat lunak, contoh : username, password, *ip address*, *mac-address*. Sedangkan menurut Zhaofeng DRM dapat ditinjau dari aspek model, teknologi dan aplikasi [10]. Tiga penelitian pertama peneletian di atas di dalamnya terdapat bagian utama dari DRM yaitu teknik autentikasi. Teknik autentikasi ini yang digunakan untuk melindungi perangkat lunak. Selanjutnya ada juga penelitian yang melakukan pengembangan DRM dengan metode Content Decryption Module (CDM)[9]. CDM Oleh karena itu teknik autentikasi ini menjadi bagian yang dikembangkan pada penelitan kami.

Salah satu teknik autentikasi yang dapat kami jadikan rujukan adalah teknik *mutual authentication* yang dibuat oleh *Philips Semiconductor* [4]. Mutual authentication adalah teknik autentikasi yang dilakukan oleh client dan server dimana keduanya saling memberikan *challenge* dan *response*. Teknik mutual authentication yang dilakukan oleh Philips semiconductor termasuk algoritma yang ringan. Philips semiconductor sebelumnya menggunakan algoritma mutual authentication antara perangkat *smart card* dan alat pembaca *smart card*. Namun, menurut kami teknik autentikasi yang digunakan oleh *Philips Semiconductor* ini dapat diadopsi sebagai alat autentikasi pada DRM perangkat lunak.

Penelitian kami adalah pembuatan DRM perangkat lunak dengan teknik *access control* dan teknik autentikasi. Fungsionalitas pertama yang dimiliki oleh DRM yang kami buat adalah *mutual authentication* antar perangkat lunak dengan server. Fungsionalitas kedua adalah enkripsi pesan yang dikirimkan antara perangkat lunak dan *server*.

II. TINJAUAN PUSTAKA

Digital Right Management (DRM) merupakan upaya perlindungan perangkat lunak dari sebuah pembajakan. Menurut penelitian [3] DRM dibagi menjadi 4 pilar yaitu:

a. *Encryption* adalah teknik mengenkripsi konten digital,
b. *Conditional access* adalah pembuatan kontrol akses ke perangkat lunak,
c. *Copy policy* mencakup pengaturan terhadap pengubahan dan duplikasi data,
d. *Identification and tracking* mencakup kontrol penyebaran penggunaan data digital.

Beberapa penelitian yang kami jadikan rujukan salah satunya adalah yang ditulis oleh Tian [1]. Tian membuat DRM dengan memanfaatkan algoritma kunci publik. Algoritma kunci publik dimanfaatkan untuk melakukan proses autentikasi. Tian membuat DRM untuk melindungi akses siaran Televisi. Tian mengenkripsi konten siaran televisi. Penelitian berikutnya adalah penelitian yang dilakukan oleh Haytham [2]. Haytham juga membuat DRM untuk melindungi konten siaran televisi. Haytham melakukan dua proses autentikasi yaitu autentikasi untuk pemilihan chanel televisi dan autentikasi untuk mendapatkan konten televise. Kemudian penelitian ketiga adalah penelitian yang dilakukan oleh Ubaidillah. Ubaidillah membuat

DRM dengan teknik Attribute Based Access Control (ABAC). Ubaidillah menggunakan banyak atribut yang dimiliki oleh komputer maupun user perangkat lunak sebagai parameter perangkat lunak.

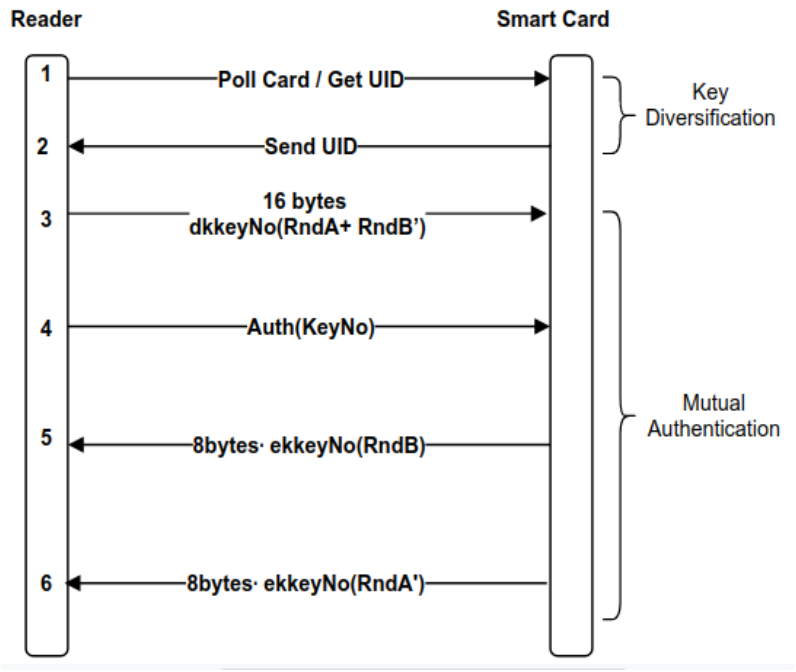
Tiga penelitian di atas menunjukkan bahwa DRM adalah hal yang sangat penting untuk melindungi akses maupun data yang melekat pada perangkat lunak. Dapat diambil kesimpulan bahwa tiga penelitian sebelumnya menggunakan teknik autentikasi dalam DRM. Dapat disimpulkan kembali teknik autentikasi merupakan bagian yang cukup banyak digunakan pada DRM.

Dengan melihat pentingnya teknik autentikasi pada DRM maka penulis mengambil teknik autentikasi dari penelitian yang dilakukan oleh Yoso [5]. Yoso menerapkan teknik autentikasi yang dibuat oleh Philips Semiconductor. Teknik autentikasi yang dilakukan oleh Philips masih digunakan hingga saat ini yaitu pada *smart card*. Contoh *smart card* buatan Philips di Indonesia adalah E-KTP, kartu BPJS Kesehatan, kartu SIM mobil dan motor. Kartu-kartu di atas menggunakan algoritma *muthual authentication* buatan Philips pula.

Beberapa kelebihan teknik autentikasi yang dibuat oleh Philips yaitu sederhana namun mampu melakukan *mutual authentication* [4]. Keunggulan teknik mutual authentication yang dilakukan oleh Philips tidak membutuhkan algoritma kunci publik. Karena tidak menggunakan algoritma kunci publik maka komputasi yang dilakukan jauh lebih ringan. Yoso pernah memanfaatkan teknik *mutual authentication* tersebut pada teknologi *smart card* [5]. Perangkat smart card yang ada di Indonesia saat ini kebanyakan menggunakan protokol komunikasi buatan *Philips Semiconductor*. Oleh karena algoritma *mutual authentication* yang dibuat oleh Philips memenuhi aspek keamanan autentikasi sekaligus ringan maka algoritma ini akan diadopsi pada DRM. Bab berikutnya akan membahas algoritma mutal authentication yang dibuat oleh Philips.

1) Philips Mutual Authentication

Berikut merupakan algoritma mutual authentication yang dibuat oleh Philips yang diimplementasikan pada *smart card* saat ini. Bahkan smart card yang digunakan di Indonesia sebagian besar menggunakan smart card buatan NXP dengan protokol buatan Philips Semiconductor.



Gambar 1. Algoritma *Mutual Authentication* oleh Philips Semiconductor.[4]

Sequence Diagam di atas adalah proses mutual authentication yang dibuat oleh Philips Semiconductor. *Mutual Authentication* ini sebelumnya diimplementasikan pada smart card buatan NXP Semiconductor.

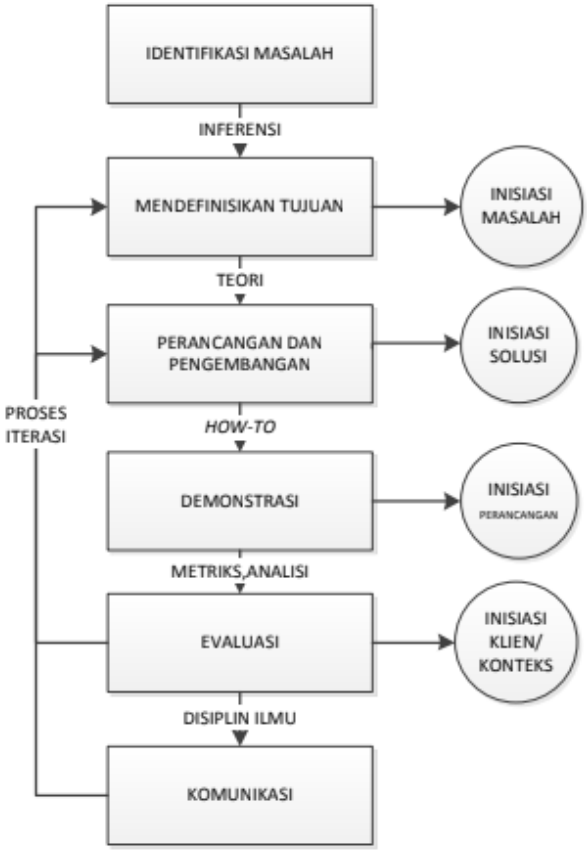
Berdasarkan sequence diagram di atas Philips memiliki 2 tahap komunikasi yaitu *key diversification* dan *mutual authentication*. Protokol ini diterapkan pada *smart card* dan *reader*-nya.

2) Tiny Encryption Algorithm (TEA)

Tiny Encription Algoritma (TEA) merupakan algoritma enkripsi kunci simetris [6]. Algoritma ini merupakan algoritma yang sangat ringan jika dibandingkan dengan algoritma lain seperti AES, DES. Oleh karena algoritma ini sangat ringan maka kami memilihnya untu diimplementasikan pada protokol yang kami buat. Berbeda dengan penerapan protokol yang dilakukan ole Philips yang mana menggunakan algoritma DES.

II. METODE PENELITIAN

Pada bab ini akan dibahas bagaimana penelitian ini akan mengacu pada sebuah metodologi. Metodologi yang digunakan dalam penelitian ini mengacu pada desain metodologi ilmiah untuk riset sistem informasi yang mencakup enam aktivitas riset. Metodologi ilmiah tersebut dikenal dengan nama *Design Science Research Methodology* (DSRM) untuk riset sistem informasi [7]. DSRM terbagi menjadi tiga tahap yaitu *problem identification, solution detail,* dan *evaluation*. Dari tiga tahap tersebut kami sisipkan beberapa tahap agar metodologi yang digunakan lebir terperinci. Metodologi yang sudah sering dipakai untuk penelitian-penelitian sejenis. DSRM untuk sistem informasi memiliki empat kemungkinan entri poin atau inisiasi aktivitas riset, yaitu orientasi masalah, orientasi solusi atau tujuan, orientasi desain dan pengembangan, serta orientasi pengguna atau konteks. Penelitian ini menggunakan entri poin yang diinisiasi oleh orientasi desain dan pengembangan.

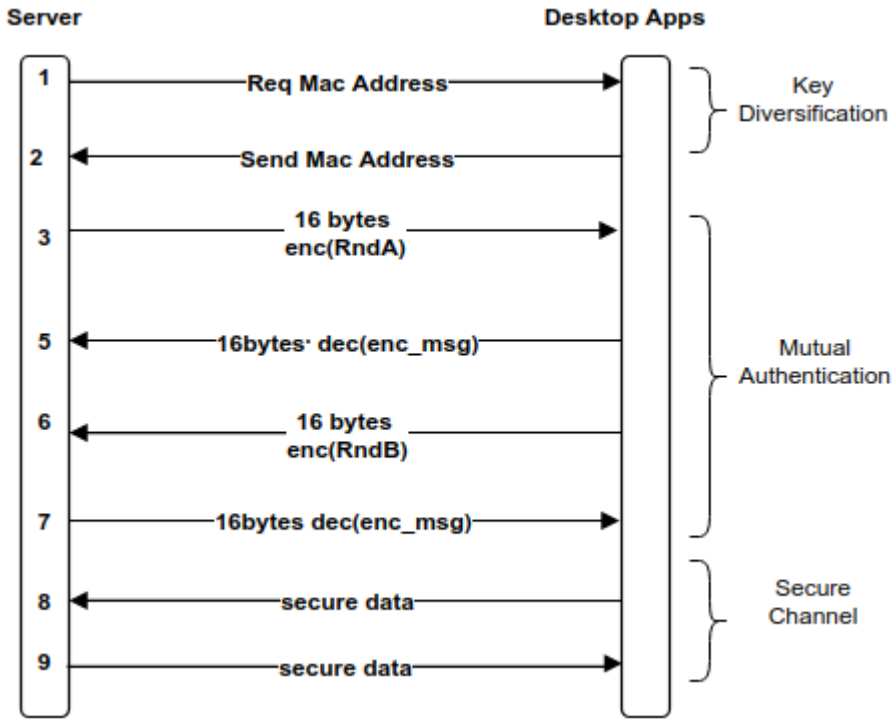


Gambar 2. Metodologi Penelitian *Design Science Research Methodology*

1. Identifikasi Masalah
   Pada tahap ini dilakukan analisis masalah yang terjadi pada *Digital Right Management* (DRM). Masalah-masalah tersebut mencakup melihat karakteristik DRM beserta pilar-pilar yang ada pada DRM.
2. Penentuan Tujuan Penelitian
   Pada tahap ini penulis menentukan tujuan penelitian. Tujuan penelitian ini adalah membangun sistem DRM untuk perangkat lunak agar terlindung dari pembajakan.
3. Perancangan dan Pengembangan
   Pada tahap ini penulis melakukan perancangan sistem DRM. DRM dibangun melekat langsung pada setiap perangkat lunak yang dibangun. DRM yang dibangun mengadopsi dan memodifikasi teknik *mutual authentication* milik Philips Semiconductor.
4. Demonstrasi dan Evaluasi
   Pada tahap ini penulis melakukan uji coba DRM yang telah dibangun. Penelitian akan dievaluasi. Hasil evaluasi DRM akan menjadi bahan penelitian selanjutnya.
5. Komunikasi
   Pada tahap ini penulis melakukan publikasi penelitian. Melalui publikasi penelitian dapat menjadi bagian evaluasi.

III. HASIL DAN PEMBAHASAN

Penelitian ini akan mengadopsi protokol di atas untuk dipasang pada *server* dan *client desktop apps*. Berikut rancangan protokol antara *server* dan *client* untuk implementasi *mutual authentication*. Protokol komunikasi di atas akan diadopsi untuk diimplementasikan pada perangkat server dan client (*desktop application*). Berikut rancangan protokol dalam hasil adopsi.



Gambar 3 Modifikasi Protokol Mutual Authentication Philips

Dari sequence diagram yang tertera di atas dapat dieketahui bahwa fitur dan aspek keamanan terbagi dalam tiga tahap yaitu *key diversification, mutual authentication,* dan *secure channel / secure data*. Penjelasan tiga fase protokol komunikasi di atas adalah sebagai berikut.

1) *Key Diversification*

Key Diversification merupakan sebuah proses menentukan kunci privat. Dalam scenario komunikasi di sini kunci privat dibuat oleh dua *server* dan *client*. Sehingga dengan proses ini maka kedua belah pihak akan memiliki kunci privat. Pada protokol yang ada pada Philips sebelumnya kunci privat ini akan dibangkitkan menggunakan parameter UID. Perancangan protokol saat ini akan menggunakan *mac address* sebagai pengganti UID. Mac address digunakan sebagai bahan proses *key diversification*. Mac address akan diambil dan diacak sedemikian rupa sehingga akan membentuk kunci baru. Selain menggunakan mac address kedua belah pihak juga menggunakan *secret stored key* untuk membangkitakan *private key*. Attacker tidak akan kecil kemungkinan untuk menemukan kunci dikarenakan attacker tidak mengetahui fungsi *key diversification*-nya. Perlu diketahui bahwa proses *key diversification* tidak melakukan pertukaran kunci. Ukuran kunci yang digunakan sebesar 128 bit. Berikut proses key diversification pada system yang kami buat. Dengan bahan ini maka setiap device yang menggunakan protokol ini akan memiliki kunci yang berbeda.

2) *Mutual* Authentication

Mutual authentication adalah proses autentikasi dua arah. Untuk perancangan protokol yang dibuat saat ini mutual authentication akan dilakukan oleh client dan server. *Client* autentikasi ke server begitu juga sebaliknya *server* melakukan autentiasi juga ke *client*. Dengan adanya fungsi ini maka *client* dan *server* tidak akan dapat melakukan transaksi dengan sembarang *device*. Setelah key diversification selesai maka proses selanjutnya adalah mutual authentication. Client dan server masing-masing saling memberikan challenge dan response. Proses mutual autentikasi yang kami buat melibatkan fungsi enkripsi dan dekripsi. Algoritma yang digunakan adalah algoritma TEA.

3) *Secure* Channel

Setelah proses mutual authentication berhasil dilakukan maka proses selanjutnya adalah pembuatan saluran pertukaran data yang aman. Komunikasi yang aman dapat dibuat dengan memanfaatkan kunci privat yang dibuat pada tahap sebelumnya. Pada bagian ini client dan server sudah dapat bertukar data terenkripsi antara client dan server.

Selanjutnya pada bagian ini kami akan menyajikan hasil penelitian. Hasil penelitian kami adalah validasi skenario protokol. Perancangan komunikasi antara client dan server dibuat menggunakan pemrograman socket. Dengan pemrograman socket ini maka client dan server akan menggunakan nomor port tertentu untuk komunikasi. Algoritma yang digunakan pada penelitian ini adalah TEA.

A. Analisis Ancaman dan Upaya Pengamanan

Dengan adanya tiga fase proses komunikasi maka berikut kami sajikan objektif keamanan yang disediakan oleh system. Kami menyajikan tabel analisis celah keamanan yang kemungkinan teradi pada sistem yang kami buat sebagai berikut.

Tabel 1. Daftar Celah dan Pengamanan

	Celah Keamanan		
	Celah Kunci Bocor	**Celah User Akses**	**Celah Pesan Bocor**
Penanggulangan	Dapat ditanggulangi dengan fungsing *key*	Dapat ditanggulangi dengan *mutual authentication*	Dapat ditanggulangi dengan *secure channel* dalam pertukaran data.

	diversification		
Pilar DRM	Pilar *Identification and Tracking*	Pilar *Conditional Access*	Pilar *Encryption*

Tabel di atas menunjukkan bahwa ada tiga celah keamanan yang mungkin terjadi antara client dan server yaitu celah kunci bocor, celah user akses, dan celah pesan bocor. Pada protokol yang kami buat tiga celah tersebut sudah kami tanggulangi. Protokol keamanan yang kami buat adalah hasil modifikasi dari protokol yang dibuat oleh Philips. Hal ini dapat diketahui dari *sequence diagram* yang kami buat. Begitu juga implemantasi yang kami lakukan tidak menggunakan smart card namun dimanfaatkan pada komunikasi *client-server*.

V. KESIMPULAN

Kesimpulan dari penelitian ini adalah perancangan protokol keamanan yang dibuat dapat dibutktikan secara matematis dan sistematis dapat melindungi komunikasi antara *client* dan *server*. Dari hasil analisis keamanan menunjukkan ada tiga potensi celah dan ancaman keamanan yaitu celah kebocoran kunci, celah kebocoran autentikasi, serta kebocoran pertukaran data. Penulis berhasil menyusun sedemikian rupa protokol sehingga dapat menanggulangi tiga celah keamanan tersebut. Tiga teknik penanggulangan tersebut adalah teknik key diversification, teknik *mutual authentication*, dan teknik *secure channel*. Ketiga fungi tahap protokol tersebut masuk ke dalam DRM untuk pilar *identification and tracking*, *conditional access*, dan *encryption*. Kelanjutan dari penelitian ini adalah pengujian *availability* dan dan performansi protokol.

DAFTAR PUSTAKA

[1] Sumit Goswami, Sudip Misra, and Mukesh Mukesh, "A replay attack resilient system for PKI based authentication in challenge-response mode for online application", 3rd International Conference on Eco-friendly Computing and Communication Systems. IEEE, (2014).
[2] Haytham Al-Feel, "Semantic-Based Digital Rights Management System for TV Broadcasting", IEEE. (2015).
[3] Ubaidillah, "Digital Rights Management with ABAC Implementation To Improve Enterprise Document Protection", IEEE, (2014)
[4] Philips Semiconductor, mifare DESFire Contactless Multi-Application IC with DES and 3DES Security MF3 IC D40. Philips. (2004)
[5] Yoso Adi Setyoko, "Security Protection Profile on Smart Card System Using ISO 15408 Case Study: Indonesia Health Insurance Agency", Sixth International Conference on ICT(ICoICT), IEEE, (2018).
[6] Derek Williams. "The Tiny Encryption Algorithm (TEA)". Columbus State University. (2008)
[7] Philipp Offermann. Olga Levina. Marten Schönherr. Udo Bub. "Outline of a Design Science Research Process". Conference Paper. ResearchGate. (2009)
[8] https://kabar24.bisnis.com/read/20200103/16/1186527/indonesia-dan-pembajakan-perangkat-lunak. Diakses pada 18 Mei 2020.
[9] Stefan Pham, Stefan Arbanowski, Stefan Kaiser. "An Open Source Open Decryption Module to improve DRM Integration with HTML5 platforms". International Symposium on Multimedia. IEEE. 2015.
[10] Zhaofeng Ma. "Digital Rights Management: Model, Technology and Application". China Communications (Volume: 14, Issue: 6, 2017). IEEE. 2017.