JUSTINDO
Jurnal Sistem dan Teknologi Informasi
http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO

E-ISSN: 25541-5735, P-ISSN: 2502-5724
Volume 6, No. 2, Agustus 2021

Evaluasi Keamanan Sistem *E-government* menggunakan Security Development Lifecycle (SDL) Threat Modelling Tool

Said Akmala[1], Imam Riadi[2], Yudi Prayudi[3]

[1,3]Universitas Islam Indonesia - Yogyakarta
[2]Universitas Ahmad Dahlan - Yogyakarta
Email: 17917129@students,uii.ac.id

(Naskah masuk: 29 Maret 2021, diterima: 16 Juni 2021, diterbitkan: 31 Agustus 2021)

ABSTRAK

Sistem informasi berupa pelayanan publik saat ini mulai berkembang cukup pesat di Indonesia, kini banyak penyajian informasi disajikan secara digital atau yang dikenal dengan *electronic government* (*e-government*). Konsep *e-government* sendiri adalah penggunakan teknologi informasi sebagai salah satu alat pemerintah untuk meningkatkan pelayanan pemerintah kepada warga negara, lembaga swasta dan lembaga pemerintah lain yang saling berinteraksi. Namun dalam penggunaan sistem *e-government* sendiri memungkinkan banyak terjadinya risiko ancaman oleh karena itu diperlukan evaluasi keamanan sistem. Penelitian ini membahas mengenai tahapan dalam melakukan evaluasi keamanan sistem menggunakan metode *Security Development Lifecycle (SDL)* yang memiliki 6 tahapan yaitu *Define, Diagram, Identify, Mitigate dan Validate*. Hasil uji menggunakan *SDL* dalam evaluasi sistem *e-government* menghasilkan suatu nilai tingkat risiko ancaman dengan menggunakan penilaian berbasis *STRIDE* dan *DREAD* dengan potensi ancaman yaitu : *spoofing* sebesar 4, *tampering* sebesar 11, *elevation of privilege* sebesar 8, *Danial of Service* sebesar 1 dan *information disclosure* sebesar 1. Hasil potensi ancaman tersebut kemudian dianalisis sehingga menghasilkan sebuah kesimpulan bahwa dalam sistem memerlukan langkah pencegahan dengan membuat *TLS* (*Transport Layer Security*) menggunakan mekanisme autentifikasi yang baik, melaukan enkripsi pada database, menggunakan *Spam Filter* dan *update* rutin sandi secara berkala. Kelebihan *SDL* yaitu bersifat pengulangan sehingga dalam pengujiannya memungkinkan untuk selalu mengevaluasi dan menguji ulang sistem untuk melakukan langkah prioritas dalam melakukan mitigasi terhadap potensi ancaman.

Kata kunci: *e-government, modelling, SDL, STRIDE, DREAD, evaluasi.*

ABSTRACT

Information systems in the form of public services are currently starting to develop quite rapidly in Indonesia, now many information presentations are presented digitally or known as electronic government (*e-government*). The concept of *e-government* itself is the use of information technology as a government tool to improve government services to citizens, private institutions and other government agencies that interact with each other. However, the use of the *e-government* sistem itself allows a lot of threat risks, therefore it is necessary to evaluate the security of the sistem. This study discusses the stages in evaluating sistem security using the Security Development Lifecycle (SDL) method which has 6 stages, namely Define, Diagram, Identify, Mitigate and Validate. The test results using SDL in evaluating the *e-government* sistem produce a threat risk level value using STRIDE and DREAD-based assessments with potential threats, namely: 4 threats of spoofing, 11 threats of tampering, 8 threats of elevation of privilege, 1 threat of Danial of Service and 1 threats of information disclosure. The results of the potential threats then analyzed to produce a conclusion that the sistem requires preventive measures by making TLS (Transport Layer Security), using a good authentication

mechanism, encrypting the database, using Spam Filters and updating passwords regularly. The advantage of SDL is that it is iterative so that in its testing it is possible to always evaluate and retest the sistem to take priority steps in mitigating potential threats.

Keywords: *e-government, modelling, SDL, STRIDE, DREAD, evaluate.*

1. PENDAHULUAN

Sistem penyajian informasi berupa pelayanan publik saat ini mulai berkembang cukup pesat baik pada sektor pemerintah maupun swasta (Ali et al., 2016). Kini banyak penyajian informasi pemerintah juga disajikan secara digital atau yang dikenal dengan *electronic government* (*e-government*). Konsep *e-government* sendiri adalah penggunakan teknologi informasi sebagai salah satu alat pemerintah untuk meningkatkan pelayanan pemerintah kepada warga negara, lembaga swasta dan lembaga pemerintah lain yang saling berinteraksi (Hayati, 2018) (Salsabila & Purnomo, 2017). Selain itu *e-government* adalah wujud aplikasi dalam pelayanan public agar membantu mempermudah dalam segala kegiatan dan urusan pemerintah sesuai dengan landasan hukum yang berlaku untuk meningkatkan tranparansi dan kepercayaan masyarakat (Kim et al., 2020). Penggunaan teknologi informasi disatu sisi banyak memberikan kemudahan bagi para penggunanya, namun disisi yang lain bisa menjadi ancaman yang datang dari berbagai sumber seperti karyawan atau serangan *hacker* yang dapat menyebabkan berbagai macam kerugian (Jouini et al., 2014). Sebuah sistem *e-government* juga harus dievaluasi dampaknya dalam hal manfaat, biaya dan risiko agar dapat dirasakan manfaatnya secara baik (Irani et al., 2008). Di Indonesia sendiri banyak sekali serangan siber yang menyerang, menurut Laporan Tahunan *Honeynet Project* tahun 2018 setidaknya ada 12.895.554 serangan yang terpantau pada 21 sensor yang terpasang . Hal ini tentu perlu menjadi sebuah perhatian agar *Threat*/ancaman yang dapat memungkinkan terjadinya eksploitasi kerentanan dalam menembus sebuah sistem keamanan (Satapathy, 2014). Untuk itu pemodelan ancaman merupakan kunci utama untuk mendapatkan potensi ancaman pada sebuah sistem (Wuyts et al., 2014) yang dapat digunakan untuk meningkatkan sistem keamanan informasi agar pelayanan publik dapat diakses secara cepat, tepat dan memberikan hasil yang akurat serta terpercaya dengan penuh pertanggungjawaban. konsep keamanan siber sendiri merupakan perlindungan dari pencurian atau kerusakan pada perangkat keras, perangkat lunak, dan data yang tersimpan di sistem (Lezzi et al., 2018). Karena dalam dunia digital, kemanan informasi adalah kunci keberhasilan implementasi sebuah sistem *e-government* (Pandya & Patel, 2017).

Dalam melakukan pencegahan terhadap risiko ancaman serangan siber banyak digunakan berbagai macam metode, termasuk mennggunakan *Threat Modelling* yang dapat digunakan untuk membantu mengidentifikasi, menganalisis ancaman dan mengembangkan langkah mitigasi (Saripalli & Walters, 2010). Dalam penelitian ini digunakan Metode *Security Development Lifecycle (SDL)* yang menggabungkan tahapan identifikasi risiko ancaman berdasarkan *STRIDE dan DREAD* (Hussain, S., Kamal, A., Ahmad, S., Rasool, G., & Iqbal, S, 2014). Dengan demikian menemukan kerentanan adalah langkah penting dan mendasar dalam analisis ancaman (Hong et al., 2019)

 p-ISSN : 2502-5724; e-ISSN : 2541-5735

STRIDE merupakan kategori sebuah ancaman dari hasil pemodelan yang telah dilakukan, *STRIDE* secara umum membagi jenis serangan yang mungkin akan ada kedalam 6 jenis serangan yaitu : *Spoofing, Tampering, Repudiation, Information disclosure, Denial of service dan Elevation of privilege* (Macher, G., Armengaud, E., Brenner, E., & Kreiner, C, 2016).

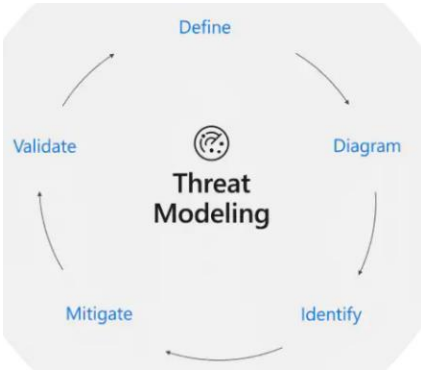
Sedangkan *DREAD* merupakan sebuah pemodelan ancaman yang digunakan untuk menilai tingkat keamanan dari sebuah sistem. Pemodelan *DREAD* dibagi menjadi lima kategori yaitu: *Damage potential, Reproducibility, Exploitability, Affected users dan Discoverability*. Nantinya kombinasi antara *STRIDE* dan *DREAD* mampu menghasilkan suatu nilai tingkat risiko ancaman sehingga memudahkan dalam melakukan prioritas perbaikan sistem (Meimer, J.D, Mackman, A, Wastell B, 2010).

2. METODE

Metode berisi menjelaskan bagaimana cara penelitian dilakukan sehingga dapat diketahui rincian tentang urutan langkah-langkah yang dibuat secara sistematis dan dapat dijadikan pedoman yang jelas dalam menyelesaikan permasalahan, membuat analisis terhadap hasil penelitian, serta kesulitan-kesulitan yang dihadapi. Adapun langkah-langkah atau tahapan-tahapan pada penelitian ini dapat dilihat pada Gambar 1

Gambar 1 Alur Metode Penelitian

Dalam melakukan identifikasi sistem *e-government* adalah dengan menentukan sistem *e-government* yang akan dipilih yaitu sistem e-monitoring Kabupaten Purbalingga, kemudian dilakukan Studi Literature yang berkaitan dengan sistem *e-government* tersebut. Pada Gambar 1 terdapat sebuah alur nomor 3 yaitu: Pemodelan Sistem sebagai langkah untuk mengidentifikasi, menilai dan memitigasi risiko ancaman (Maheshwari, V., & Prasanna, M, 2017). Kemudian pemodelan dilakukan menggunakan Metode Security Development Lifecycle (SDL) sebelum melakukan analisis Ancaman dan Kesimpulan yaitu dengan langkah pada Gambar 2 sebagai berikut :



Gambar 2 Tahap Security Development Lifescyle (SDL)

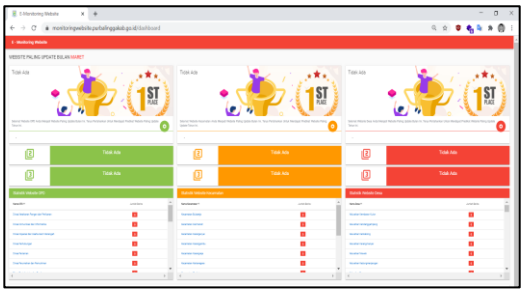
Dalam tahap *SDL* terpadat tahap *identify* yang berdasarkan klasifikasi *STRIDE* yang bersifat otomatis (Tatam, etc. 2021) (Navas & Beltrán, 2019) dan tahap *Rating* Ancaman berdasarkan *DREAD* yang akan disajikan dalam bentuk nilai berdasarkan tingkat ancaman yaitu *High* (3), *Medium* (2) dan *Low* (1) (Meimer, J.D, Mackman, A, Wastell B, 2010). Dalam penyajian data risiko ancaman dikatakan baik apabila disajikan sebagai angka kardinal atau persentase, bukan dengan label kualitatif seperti tinggi, sedang dan rendah (Burnap, 2019). Tahap Rating berdasarkan DREAD digunakan sebagai analisis untuk penanggulangan ancaman pada sistem. (Omotosho et al., n.d, 2020)

3. HASIL DAN PEMBAHASAN

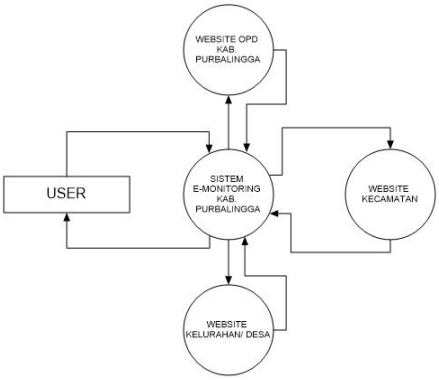
Hasil dan Pembahasan yang dilakukan meliputi :

A. Identifikasi Sistem *e-government*

Identifikasi sistem *e-government* dilakukan dengan melakukan wawancara dan analisis sistem *e-monitoring* pada : https://monitoringwebsite.purbalinggakab.go.id/. Web aplikasi tersebut dibuat untuk melakukan monitoring dan memudahkan pengelolaan informasi di Kabupaten Purbalingga, Jawa Tengah yang disajikan dalam satu tampilan dan sudah saling terintegrasi. Dalam web *e-monitoring* tersebut berisi tentang informasi berita di Kabupaten Purbalingga yang terintergasi dengan 25 Website Organisasi Perangkat Daerah (OPD), 14 Website Kecamatan, 121 Website Desa/ Kelurahan. Tampilan Website dapat dilihat pada Gambar 3 berikut gambaran Sistem E-Monitoring pada Gambar 4.



Gambar 3 Tampilan Website E-monitoring



Gambar 4 Gambaran Sistem E-monitoring

1) Detail Sistem *E-government*

Sistem *e-monitoring* Kabupaten Purbalingga memiliki manajemen sistem seperti pada Tabel 1 sebagai berikut :

Tabel 1 Manajemen sistem e-monitoring

Jenis	Ket.
Bahasa Pemrograman	Node.js
Web Servers	Nuxt.js
Web Framework	Nuxt.js
CDN	Cloudflare
XmlHttpRequest	stat-opd
	stat-kecamatan
	Stat-desa
	Stat-year
Web API	Available
Database	Available

B. Pemodelan Sistem (SDL Based)

Pemodelan sistem dilakukan menggunakan metode *Security Development Lifecycle (SDL)* dengan menggunakan aplikasi *Microsoft Threat Modeling Tool*. Setelah melakukan identifikasi sistem e-monitoring, selanjutkan adalah melakukan pemodelan sistem berdasarkan hasil identifikasi sistem tersebut. Terdapat setidaknya enam komponen utama yaitu seperti pada Tabel 2 yaitu : *User, Browser, Web Aplication, Web API, Web Service* dan *Database.*

Tabel 2 Komponen Pemodelan Sistem

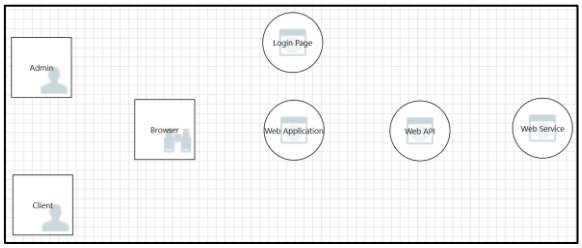
Komponen	Keterangan
User	Terdiri dari admin dan client
Browser	Software yang digunakan untuk mengakses Web
Web Aplication	Web Utama yang akan dianalisis yaitu : https://monitoringwebsite.purbalinggakab.go.id/
Login Page	Login page for Admin
Web API	Data Hasil dari Web Service, data yang ditampilkan dalam bentuk JSON
Web Service	Jembatan untuk memudahkan mengakses Database

p-ISSN : 2502-5724; e-ISSN : 2541-5735

Database	Tempat penyimpanan data, untuk database yang digunakan adalah mongoDB (noSQL Database)

1) Membuat Pemodelan Komponen Utama

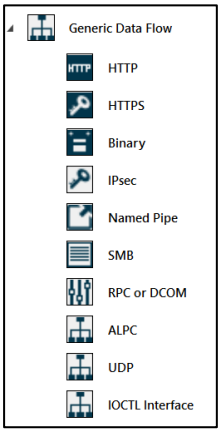
Komponen utama dari web e-monitoring https://monitoringwebsite.purbalinggakab.go.id/ dapat terlihat pada Gambar 5 yang terdiri dari *Human User* (*Admin* dan *Client*), *Browser, Web Application (e-monitoring), Login Page, Web API, Web Service* dan *Database.*



Gambar 5 Tahap 1 Pembuatan Komponen Utama

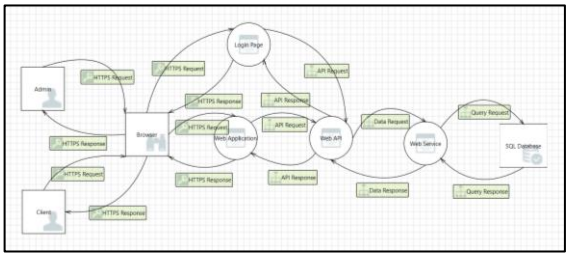
2) Membuat Jenis *Generic Data Flow*

Membuat jenis *generic data flow* yang yang saling menghubungkan pada komponen utama yang telah dibuat. Jenis *Generic Data Flow* yang tersedia pada aplikasi *Microsoft Threat Modeling* (Satapathy, 2014) ada pada Gambar 6 yaitu:



Gambar 6 Jenis Generic Data Flow yang tersedia

Adapun *Generic Data Flow* yang digunakan untuk komponen utama pada pemodelan sistem *e-monitoring* yaitu : *HTTPS, Generic Data Flow* dan *UDP* yang digambarkan request dan response seperti pada Gambar 7 sebagai berikut :



Gambar 7 Tahap 2 Pembuatan Jenis Generic Data Flow

Penjelasan Gambar 7 dalam Pembuatan Jenis *Generic Data Flow* dapat dilihat pada Tabel 3 yaitu :

Tabel 3 Penjelasan Human User

Human User	**Data Flow**
Admin	1) Admin melakukan HTTPS Request ke Browser yang diteruskan ke Login Page. Apabila request sebagai Admin tidak berhasil maka akan segera dilakukan response dan tidak bisa melanjutkan ke proses berikutnya. Karena login page berisi tentang hak akses sebagai admin dalam melakukan manajemen/ pengelolaan pada sistem e-monitoring.
	2) Dari Login page kemudian melakukan API Request ke Web API
	3) Dari Web API kemudian melakukan Data Request ke Web Service
	4) Dari Web Service kemudian melakukan Query Request ke SQL Database yang kemudian akan memberikan response sesuai dengan request yang dilakukan oleh Admin.
Client	1) Client melakukan HTTPS Request ke Web Application

yaitu sistem e-monitoring. Request tersebut bisa berarti tentang pencarian informasi seperti: informasi Organisasi Perangkat Daerah (OPD), Informasi Kecamatan, Informasi Desa/ Kelurahan, Statistik Rata-rata postingan.

2) Dari Web Application tersebut kemudian melakukan API Request ke Web API
3) Dari Web API kemudian melakukan Data Request ke Web Service
4) Dari Web Service kemudian melakukan Query Request ke SQL Database yang kemudian akan memberikan response sesuai dengan request yang dilakukan oleh Client.

C. Hasil Potensi Ancaman

Setelah melakukan tahap Pemodelan, didapatkan hasil potensi ancaman yaitu seperti pada Tabel 4 :

Tabel 4 Hasil Potensi Ancaman

id	Title	Category
1	Spoofing the Browser External Entity	Spoofing
2	Cross Site Scripting	Tampering
3	Elevation Using Impersonation	Elevation Of Privilege
4	Spoofing the Browser External Entity	Spoofing
5	Cross Site Scripting	Tampering
6	Elevation Using Impersonation	Elevation Of Privilege
7	Login Page Process Memory Tampered	Tampering
8	Elevation Using Impersonation	Elevation Of Privilege
9	Web API Process Memory Tampered	Tampering
10	Cross Site Scripting	Tampering
11	Elevation Using Impersonation	Elevation Of Privilege
12	Web Application Process Memory Tampered	Tampering
13	Elevation Using Impersonation	Elevation Of Privilege
14	Web API Process Memory Tampered	Tampering
15	Cross Site Scripting	Tampering
16	Elevation Using Impersonation	Elevation Of Privilege
17	Web API Process Memory Tampered	Tampering
18	Elevation Using Impersonation	Elevation Of Privilege
19	Web Service Process Memory Tampered	Tampering
20	Elevation Using Impersonation	Elevation Of Privilege
21	Spoofing of Destination Data Store SQL Database	Spoofing
22	Potential SQL Injection Vulnerability for SQL Database	Tampering
23	Potential Excessive Resource Consumption for Web Service or SQL Database	Denial Of Service
24	Spoofing of Source Data Store SQL Database	Spoofing
25	Weak Access Control for a Resource	Information Disclosure

D. Analisis Ancaman

Setelah didapatkan hasil 25 potensi ancaman pada Tabel 4 maka selanjutnya dilakukan rating terhadap potensi ancaman tersebut menggunakan metode *DREAD*. Rating dengan hasil pada Tabel 5 sebagai berikut:

Tabel 5 DREAD Rating

Threat	D	R	E	A	D	Rating
Spoofing the Browser External Entity	3	2	1	3	1	10
Cross Site Scripting	1	2	2	3	1	9
Elevation Using	2	2	1	1	2	8

p-ISSN : 2502-5724; e-ISSN : 2541-5735

Impersonation						
Spoofing the Browser External Entity	3	2	1	3	1	10
Cross Site Scripting	1	2	2	3	1	9
Elevation Using Impersonation	2	2	1	1	2	8
Login Page Process Memory Tampered	3	1	1	3	1	9
Elevation Using Impersonation	2	2	1	1	2	8
Web API Process Memory Tampered	2	2	2	3	2	11
Cross Site Scripting	1	2	2	3	1	9
Elevation Using Impersonation	2	2	1	1	2	8
Web Application Process Memory Tampered	3	2	2	3	1	11
Elevation Using Impersonation	2	2	1	1	2	8
Web API Process Memory Tampered	2	2	2	3	2	11
Cross Site Scripting	1	2	2	3	1	9
Elevation Using Impersonation	2	2	1	1	2	8
Web API Process Memory Tampered	2	2	2	3	2	11
Elevation Using Impersonation	2	2	1	1	2	8
Web Service Process Memory Tampered	2	2	2	3	2	11
Elevation Using Impersonation	2	2	1	1	2	8
Spoofing of Destination Data Store SQL Database	3	2	1	3	1	10
Potential SQL Injection Vulnerability for SQL Database	2	2	1	1	1	7
Potential Excessive Resource Consumption for Web Service or SQL Database	1	1	1	1	1	5
Spoofing of Source Data Store SQL Database	3	2	1	3	1	10
Weak Access Control for a Resource	2	2	2	2	1	9
Spoofing the Browser External Entity	3	2	1	3	1	10
Cross Site Scripting	1	2	2	3	1	9
Elevation Using Impersonation	2	2	1	1	2	8

DREAD : (3)High; (2)Medium; (1)Low.
Rating : (12-15) High; (8-11)Medium; (5-7) Low.

E. Nilai Risiko Ancaman

Untuk mengetahui Nilai Risiko Ancaman maka digunakan Rumus (Meimer, J.D, Mackman, A, Wastell B, 2010) :

*Risk = Probability * Damage Potential(10)*

Risk = Risiko

Probability = Jumlah jenis ancaman yang sama

Damage Potential = bernilai 10

Kemudian menghasilkan nilai Risiko Ancaman seperti yang ada pada Tabel 6 berikut ini :

Tabel 6 Nilai Risiko Ancaman

Jenis Ancaman	Probability	Damage Potential	Nilai

Spoofing	4	10	40
Tampering	11	10	110
Elevation of Privilege	8	10	80
Denial of Service	1	10	10
Information Disclosure	1	10	10

F. Mitigasi Ancaman

Dalam melakukan mitigasi ancaman dilakukan langkah analisa terhadap 25 serangan yang terbagi kedalam lima jenis serangan yaitu : *Spoofing, Tampering, Elevation of Privilege, Denial of Service dan Information Disclosure*.

Tabel 7 Mitigasi Ancaman 1

Deskripsi Ancaman	**Spoofing the Browser External Entity**
Target Ancaman	Browser
Risk rating	High
Teknik Serangan	Browser mungkin dipalsukan oleh penyerang dan ini dapat mengakibatkan akses tidak sah ke Halaman Login.
Penanggulangan	Jangan gunakan mekanisme autentikasi standar untuk mengidentifikasi entitas eksternal.

Adapun ringkasan mitigasi yang dapat dilakukan untuk mencegah terjadinya serangan pada web e-monitoring yaitu dengan:

1) Membuat *TLS (Transport Layer Security)* untuk mencegah terjadinya serangan *SQL injection*.
2) Tidak menggunakan mekanisme autentifikasi yang bersifat standar (harus dilakukan enkripsi dan autentifikasi secara baik).
3) Menggunakan *Spam Filter*.
4) Update rutin sandi secara berkala.
5) Melindungi data dari *DDoS*.

Beberapa langkah mitigasi ancaman juga sudah dilakukan pada web *e-monitoring* seperti menggunakan enkripsi, proteksi database.

4. KESIMPULAN

Kesimpulan yang dapat diambil berdasarkan hasil evaluasi keamanan sistem *e-government* yaitu: Jurnal ini membahas tentang Evaluasi Keamanan Sistem *e-government* yang dapat dilakukan menggunakan metode *Security Development Lifecycle (SDL)* dengan mengikuti tahapan yang ada. Berdasarkan hasil pengujian sistem *e-government* masih terdapat beberapa Risiko Ancaman yang ada pada website *e-monitoring* namun masih bisa untuk dilakukan Langkah mitigasi. Beberapa langkah mitigasi ancaman juga sudah dilakukan pada web *e-monitoring* untuk mengamankan data yang ada seperti pencegahan terhadap *DDos* menggunakan *Cloudflare* serta menyembunyikan *login page*.

DAFTAR PUSTAKA

Ali, O. A., Wahbi, T. M., & Osman, I. M. (2016). *E-government* Security Models. International Journal of Computer Applications Technology and Research, 5(7), 439–442. https://doi.org/10.7753/ijcatr0507.1004

Burnap, Pete (2019). Risk Management & Governance Knowledge Area.

Hayati. (2018). Implementasi *E-government* Pada Pemerintah Daerah Kabupaten Bantul Yogyakarta. December, 1–23.

Hong, J. B., Nhlabatsi, A., Kim, D. S., Hussein, A., Fetais, N., & Khan, K. M. (2019). Sistematic identification of threats in the cloud: A Survey.

Computer Networks, *150*, 46–69. https://doi.org/10.1016/j.comnet.2018.12.009

Hussain, S., Kamal, A., Ahmad, S., Rasool, G., & Iqbal, S. (2014). Threat Modelling Methodologies: a Survey. Sci.Int.(Lahore), 26(4), 1607–1609.

Irani, Z., Love, P. E. D., & Jones, S. (2008). Learning lessons from evaluating eGovernment: Reflective case experiences that support transformational government. *Journal of Strategic Information Sistems*, *17*(2), 155–164. https://doi.org/10.1016/j.jsis.2007.12.005

Jouini, M., Rabai, L. B. A., & Aissa, A. Ben. (2014). Classification of security threats in information sistems. Procedia Computer Science, 32, 489–496.

Kim, K., Cho, K., Lim, J., Jung, Y. H., Sung, M. S., Kim, S. B., & Kim, H. K. (2020). What's your protocol: Vulnerabilities and security threats related to Z-Wave protocol. *Pervasive and Mobile Computing*, *66*(2018), 101211. https://doi.org/10.1016/j.pmcj.2020.101211

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry*, *103*, 97–110. https://doi.org/10.1016/j.compind.2018.09.004

Macher, G., Armengaud, E., Brenner, E., & Kreiner, C. (2016). Threat and Risk Assessment Methodologies in the Automotive Domain. Procedia Computer Science, 83, 1288–1294. https://doi.org/10.1016/j.procs.2016.04.268

Maheshwari, V., & Prasanna, M. (2017). Integrating risk assessment and threat modeling within SDLC process. Proceedings of the International Conference on Inventive Computation Technologies, ICICT 2016, 1(March). https://doi.org/10.1109/INVENTIVE.2016.7823275

Meimer, J.D, Mackman, A, Wastell B. (2010). Chapter 3 – Threat Modeling https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)?redirectedfrom=MSDN (diakses tanggal 4 Januari 2020).

Navas, J., & Beltrán, M. (2019). Understanding and mitigating OpenID Connect threats. *Computers and Security*, *84*, 1–16. https://doi.org/10.1016/j.cose.2019.03.003

Omotosho, A, … B. A. H.-J. of A., & 2019, undefined. (n.d.). Threat modeling of Internet of Things health devices. Taylor & Francis. Retrieved January 6, 2020, from https://www.tandfonline.com/doi/abs/10.1080/19361610.2019.1545278

Pandya, D. C., & Patel, D. N. J. (2017). Study and analysis of E-Governance Information Security (InfoSec) in Indian Context. *IOSR Journal of Computer Engineering*, *19*(01), 04–07. https://doi.org/10.9790/0661-1901040407

Salsabila, L., & Purnomo, E. P. (2017). Establishing and Implementing Good Practices *E-government* (A Case Study : *e-government* Implementation between Korea and Indonesia). In Asean/ Asia Academic Society International Conference (Aasic) (Vol. 5, pp. 221–229).

Saripalli, P., & Walters, B. (2010). QUIRC: A quantitative impact and risk assessment framework for cloud security. Proceedings - 2010 IEEE 3rd International Conference on Cloud Computing, CLOUD 2010, 280–288.

https://doi.org/10.1109/CLOUD.2010.22

Satapathy, S. R. (2014). Threat Modeling in Web Applications. June, 87. http://ethesis.nitrkl.ac.in/5793/1/E-9.pdf

Tatam, Mat. Shanmugam, Bharanidharan, Kannoorpatti S. (2021). A review of Threat Modelling Approaches for APT-Style Attacks. Elsevier Ltd. 2405-8440.

Wuyts, K., Scandariato, R., & Joosen, W. (2014). Empirical evaluation of a privacy-focused threat modeling methodology. *Journal of Sistems and Software*, *96*, 122–138. https://doi.org/10.1016/j.jss.2014.05.075