Analisis Penerapan Aspek Keamanan Informasi CIA Triad Pada Sistem Informasi Akademik

Nurmi Hidayasari[1], Kasmawi[2], Mansur[3], Putri Nuranisa[4], M. Iqbal Husaini[5]
Jurusan Teknik Informatika Politeknik Negeri Bengkalis
nurmihidayasari@polbeng.ac.id[1], kasmawi@polbeng.ac.id[2], mansur@polbeng.ac.id[3],
putrinuranisaaa044@gmail.com[4], dovikaloo262@gmail.com[5]

Abstract

Threats that often attack information systems such as data leakage, credentials, phishing, web-based attacks, malware attacks, cracking, carding and etc. These types of crimes can certainly be prevented and handled which is the responsibility of the company/organization. Information security is an effort to protect information assets from potential threats. Information security indirectly ensures business continuity, reduces emerging risks, and makes it possible to optimize return on investment. The CIA Triad Information Security aspect in information and data systems is very important as a guideline or basic framework, because in it there are indicators in preventing Cyber Crime. Politeknik Negeri Bengkalis (Polbeng) as one of the State Vocational Universities in Indonesia already uses SiakadCloud, a SEVIMA product as an integrated academic management information system. In addition, SEVIMA also claims that SIAKADCloud is a secure system. However, so far it has not been possible to ascertain the extent of its security. It is also necessary to know whether in its implementation SiakadCloud has implemented basic security standards in accordance with the CIA Triad, namely Confidentiality, Integrity, and Availability. To find out the application of Confidentiality do Block Direct, To find out the application of Integrity do User and Data filtering checks: user level division, while to find out the application of Availability do authentication.

Keywords : Information security, CIA Triad, Confidentiality, Integrity, Availability

1. PENDAHULUAN

Keamanan informasi merupakan semua pedoman, aturan, *best practice*, praktik untuk melindungi kerahasiaan, ketersediaan dan integritas data serta mencegah akses, penggunaan, modifikasi, pencatatan, dan penghancuran informasi yang tidak sah. Sebenarnya, keamanan informasi tidak hanya bisa diterapkan pada TI saja, akan tetapi perusahaan/organisasi harus memiliki suatu pemahaman agar ketika terdapat suatu masalah yang muncul, perusahaan/organisasi dapat secara cepat dan tepat menanganinya. Dengan demikian, kebutuhan akan keamanan informasi dapat terpenuhi melalui pengelolahan secara menyeluruh di setiap aspek perusahaan/organisasi.

Dengan adanya pemahaman yang baik tentang keamanan informasi, serta penerapan yang tepat dan sesuai dengan standar dan peraturan yang berlaku, maka perusahaan/organisasi dapat meminimalisir adanya masalah atau risiko sistem yang muncul dengan lebih baik, lebih cepat dan sesuai. Dalam menerapkan Keamanan Informasi, perusahaan/organiasasi harus memperhatikan 3 aspek yaitu *Confidentially*, *Integrity*, dan *Availability* (CIA) (Harahap et al., 2023). Pada umumnya ketika serangan, masalah, risiko yang mengancam keamanan informasi muncul, maka setidaknya terdapat salah satu dari aspek CIA yang akan menjadi target dari serangan tersebut.

Menurut Sarno dan Iffano Keamanan informasi merupakan upaya untuk melindungi aset informasi dari potensi ancaman. Keamanan informasi secara tidak langsung memastikan kelangsungan bisnis, mengurangi risiko yang muncul, dan memungkinkan untuk

mengoptimalkan laba atas investasi. CIA Triad dalam sistem informasi dan data sangat penting dijadikan pedoman atau dasar kerangka kerja, karena didalamnya terdapat indikator dalam pencegahan terjadinya Cyber Crime yang dapat merugikan organisasi atau perusahaan dan merupakan dasar di antara program program keamanan yang dikembangkan. Ketiga elemen tersebut merupakan mata rantai yang saling berhubungan dalam konsep *information protection* (Puriwigati, 2020).

Mengamankan sistem informasi secara umum dapat dikategorikan menjadi dua jenis, pencegahan dan penganan atau perbaikan. Usaha pencegahan dilakukan agar sisten informasi tidak memiliki celah keamanan, sedangkan usaha perbaikan dilakukan apabila celah keamanan dieksploitasi. Pengamanan dapat dilakukan dari beberapa layar yang berbeda. Seperti, layar transport dapat digunakan *Secure Socket Layer* (SSL). Secara fisik, dapat juga dilindungi dengan menggunakan *firewall* yang melindungi sistem dengan jaringan internet.

Sistem Informasi Akademik yang berbasis web (SIAKAD CLOUD) bertujuan untuk mempermudah seluruh elemen yang ada di kampus baik dosen maupun mahasiswa untuk mendapatkan informasi yang diperlukan, seperti jadwal dalam melaksanakan kuliah ataupun jadwal Ujian Tengah Semester (UTS) dan Ujian Akhir Semester (UAS) serta semua informasi kampus lainnya (Miati & Setiawan, 2022).

Politeknik Negeri Bengkalis sebagai salah satu Perguruan Tinggi Vokasi Negeri di Indonesia sudah menggunakan SIAKADCloud, produk SEVIMA sebagai sistem informasi manajemen akademik yang terintegrasi. Selain itu SEVIMA juga mengklaim bahwa SIAKADCloud merupakan sistem yang aman. Namun, sejauh ini belum dapat dipastikan sejauh mana keamanannya.

Perlu diketahui juga apakah dalam implementasinya SiakadCloud sudah menerapkan standar keamanan dasar seuai dengan CIA Triad. Oleh karena itu, penelitian ini akan melakukan analisis penerapan aspek keamanan informasi CIA Triad untuk mengukur sejauh mana keamanan yang dimiliki oleh SiakadCloud Politeknik Negeri Bengkalis (Polbeng).

Penelitian ini berfokus pada analisa aspek keamanan CIA Triad pada SIAKADCloud Polbeng. Aspek CIA Triad terdiri dari *Confidentiality* meliputi Block Direct, yaitu adanya verifikasi *username* dan *password*. *Integrity*, meliputi filterisasi data dan *user*, dengan membedakan hak akses pengguna sesuai dengan level yang dipilih. Serta *Availibility* yang meliputi autentikasi yaitu tersedianya database yang diperolehkan untuk mengakses data. Penelitian ini dilakukan untuk mengetahui sejauh mana keamanan yang dimiliki oleh SIAKADCloud Polbeng sebagai sistem informasi utama Perguruan Tinggi, apakah sudah memenuhi standar indeks keamanan informasi yang sesuai dengan aspek CIA Triad.

2. TINJAUAN PUSTAKA

Jenis keamanan informasi dapat dibagi menjadi beberapa bagian berikut (Whitman & Mattord, 2011) :

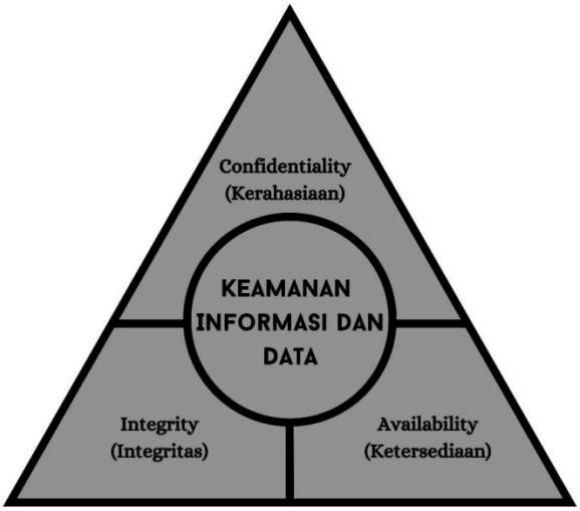
1) *Physical security*
2) *Personal security*
3) *Operational security*
4) *Communications security*
5) *Network security*

Informasi merupakan salah satu aset penting dari perusahaan. Perusahaan melakukan pengolahan terhadap informasi, kemudian hasilnya disimpan dan dibagikan. Keamanan sistem informasi terdiri dari perlindungan terhadap aspek-aspek berikut ini (Puriwigati, 2020):

a. ***Confidentially* atau Kerahasiaan** adalah aspek yang menjamin adanya kerahasiaan data dan sumber informasi. Perlu ada kepastian bahwa suatu informasi hanya dapat di akses oleh orang yang berwenang atau punya hak akses untuk menjamin kerahasiaan informasi yang dikirim.

b. ***Integrity* atau Integritas** adalah aspek yang menjamin bahwa informasi tidak dapat diubah tanpa seizin pihak berwenang, menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integritas.
c. ***Availability* atau Ketersediaan** adalah aspek yang menjamin bahwa informasi akan tersedia saat dibutuhkan oleh pihak berwenang atau yang memiliki hak akses dan memastikan pengguna yang berhak tersebut dapat mengakses informasi

Sumber lain menyebutkan bahwa aspek keamanan sistem informasi melingkupi 4 aspek. Grafinkel mengemukakan bahwa keamanan komputer melingkupi 4 aspek, yaitu *privacy*, *integrity*, *authentication* dan *availability*. Selain keempat hal di atas, masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic commerce*, yaitu *access control* dan *non-repudiation*. Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 4 Tahun 2016 Tentang Sistem Manajemen Pengamanan Informasi, Pasal 1 Butir 6 berbunyi, "Keamanan Informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) informasi." (Wijatmoko, 2020)



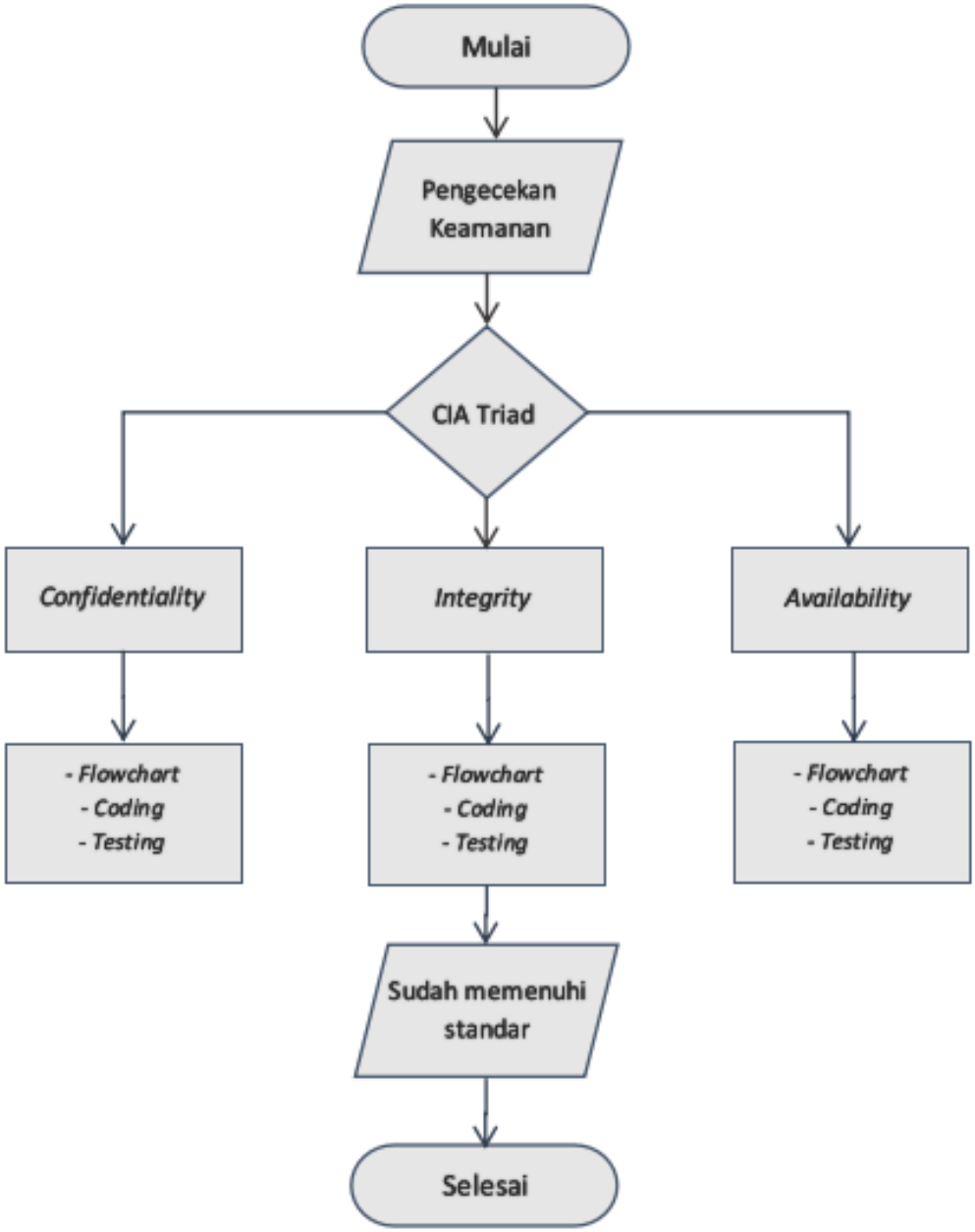
Gambar 1. CIA Triad keamanan informasi dan data
Sumber: Harahap et al., 2023

Contoh dari keamanan informasi antara lain (Puriwigati, 2020):

a. ***Physical security*** adalah keamanan informasi yang memfokuskan pada strategi untuk mengamankan individu atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman yang meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
b. ***Personal security*** adalah keamanan informasi yang berhubungan dengan keamanan personil. Biasanya saling berhubungan dengan ruang lingkup physical security.
c. ***Operasional security*** adalah keamanan informasi yang membahas bagaimana strategi suatu organisasi untuk mengamankan kemampuan organisasi tersebut untuk beroperasi tanpa gangguan
d. ***Communication security*** adalah keamanan informasi yang bertujuan mengamankan media komunikasi, teknologi komunikasi serta apa yang masih ada di dalamnya. Serta kemampuan untuk memanfaatkan media dan teknologi komunikasi untuk mencapai tujuan organisasi.
e. ***Network security*** adalah keamanan informasi yang memfokuskan pada bagaimana pengamanan peralatan jaringannya, data organisasi, jaringan dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

3. METODE PENELITIAN

Metode penelitian yang digunakan pada penelitian ini adalah mengacu pada aspek keamanan informasi CIA Triad. Tahap-tahap pengerjaan dapat dilihat pada Gambar 2.



Gambar 2. Tahapan evaluasi dengan aspek CIA Triad

Penelitian dilaksanakan di Laboratorium Keamanan Informasi Politeknik Negeri Bengkalis. Penelitian ini menggunakan model penilitian kualitatif studi kasus untuk mengetahui penerapan aspek keamanan CIA Triad pada SIAKADCloud. Parameter pengukuran yang digunakan sesuai standar CIA Triad dengan melakukan pengamatan pada SIAKADCloud langsung. Rancangan penelitian diawali dengan pengecekan aspek keamanan informasi *confidentiality*, *integrity* dan terakhir *availability*. Penelitian ini menggunakan teknik observasi. Sumber data adalah data-data yang digunakan dalam penelitian ini, yaitu data yang bersumber dari referensi, seperti buku, artikel/paper ilmiah, laporan, *survey* serta sumber data lain yang ada kaitannya dengan penelitian yang dilakukan. Teknik analisis data yang dilakukan menggunakan teknik analisis data secara kualitatif untuk menganalisis hasil

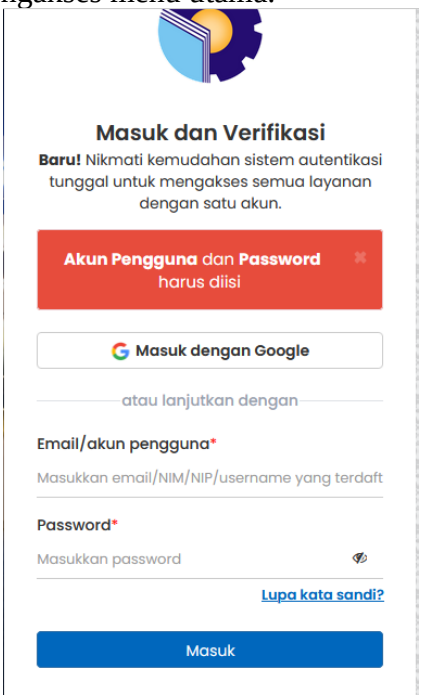
dari penerapan CIA Triad. Hasil ini akan digunakan sebagai acuan untuk mengevaluasi sistem jika dibutuhkan.

4. HASIL PENELITIAN DAN PEMBAHASAN

Penelitian ini melakukan analisa penerapan aspek keamanan informasi, yaitu *confidentiality*, *integrity* dan terakhir *availability*, melakukan pengamatan pada SIAKADCloud langsung. Langkah-langkah penelitian dan hasil yang dicapai dijelaskan sebagai berikut:

4.1. Aspek *Confidentiality*

Pada tahap ini melakukan Block Direct, di mana pada halaman *login* akan dilakukan pengecekan verifikasi *username* dan *password*. Jika data yang dimasukkan salah atau kosong apa yang akan terjadi pada sistem. Kemudian melihat isi *coding* dan melakukan *testing* uji coba terhadap *coding* tersebut. Sesuai dengan rancangan, pengguna yang mencoba masuk ke dalam sistem harus melewati halaman verifikasi yang berisi nama dan kata sandi. Jika nama pengguna dan kata sandi kosong atau salah, maka akan memberikan peringatan, dapat dilihat pada Gambar 3. Jika nama pengguna dan kata sandi sudah sesuai dan terdaftar, maka pengguna dapat masuk dan mengakses menu utama.



Gambar 3. Peringatan pada sistem jika salah masukan

```
<form method="post">
                                <div class="alert alert-danger alert-dismissable">
                <button type="button" class="close" data-dismiss="alert" aria-hidden="true">&times;</button>
                <strong>Akun Pengguna</strong> dan <strong>Password</strong> harus diisi                                    </div>
                            <div class="alert alert-danger alert-dismissable temp-error-xhr" style="display:none;">
        <button type="button" class="close" data-dismiss="alert" aria-hidden="true">&times;</button>
        <span id="error-msg"></span>
    </div>

    <div class="login">
```

Gambar 4. Kode sumber peringatan

4.2. Aspek *Integrity*

Pada aspek ini melakukan pengecekan filterisasi Pengguna dan Data: pembagian level pengguna. Untuk pengecekan, diharuskan memasukan nama pengguna, kata sandi serta memilih level pengguna di mana hal tersebut bertujuan untuk membedakan akses pengguna

sesuai level yang dipilih, setelah itu pengguna akan diarahkan ke halaman menu utama sesuai dengan level yang sudah ditentukan serta data yang di-filterisasi untuk mencegah terekspos-nya data secara menyeluruh kepada pihak yang tidak memiliki wewenang, sehingga data menjadi lebih terlindungi dan kebocoran data pun dapat dikurangi dan dihindari.

```
                        <li class="user-body">
            <form id="form_hakakses" method="post" action="/siakad/home">
                <div class="input-group">
                    <select name="hakakses" id="hakakses" class="col-sm-9 form-control input-sm">
                                                                    <option value="KA:57302"  selected>
                                Ka. Prodi                                                   </option>
                                                                    <option value="dosen:57302" >
                                Dosen                                                       </option>
                                                            </select>
                    <div class="input-group-btn">
                        <input type="submit" class="btn btn-warning btn-flat btn-sm" value="Pilih">
                    </div>
                </div>
                <input type="hidden" name="act" value="chgrole">
            </form>
        </li>

    <!-- Menu Footer-->
    <li class="user-footer">
```

Gambar 5. Kode sumber pembagian hak akses

```
cript type="text/javascript">
  main = document.getElementById('main_cont');
  var e = window,
      a = 'inner';
  if (!('innerHeight' in window)) {
      a = 'client';
      e = document.documentElement || document.body;
  }
  viewport = e[a + 'Height'];
  content = main.offsetHeight;
  if ((viewport - content) < 20) {
      main.setAttribute("style", "margin-top:" + 20 + "px;margin-bottom:20px");
  } else {
      main.setAttribute("style", "margin-top:" + ((viewport - content) / 2) + "px;margin-bottom:20px");
  }

  var last;
  var now;

  $(function() {

      $("#oldpass").focus();

      if (window.localStorage.getItem('reqPermission') === '1') {
          window.localStorage.setItem('reqPermission', '0');
      }
  });

  function goToModul(url) {
      window.open(url);
  }

  function openContent(id) {
      if (id != "") {
          last = now;
          now = id;
          window.location.hash = id;
          $("#" + last).addClass('hide');
          if (last != '')
              $("." + last).removeClass('active');
          $("#" + now).removeClass('hide');
          $("." + now).addClass('active');
```

Gambar 6. Kode sumber *filtering* data dan pengguna

Kode sumber yang digunakan adalah dengan menggunakan cabang *if*. Di sini, jika kata sandi yang dimasukkan cocok dengan kata sandi yang terdaftar di basis data, maka sistem selanjutnya akan dijalankan. Di mana nama pengguna = nama pengguna, kata sandi = kata sandi, dan level = level, berdasarkan masukkan pengguna, mengidentifikasi apakah program mengidentifikasi pengguna sebagai Dosen biasa atau Dosen dengan Jabatan Struktural (seperti, Direktur, Wakil Direktur, Ketua Jurusan, Koor. Prodi, dll). Pengguna sebagai tendik maupun sebagai mahasiswa dan menjalankan program untuk mengambil pengguna.

4.3. Aspek *Availability*

Dengan melakukan autentikasi yaitu tersedianya basis data yang diperolehkan untuk mengakses data. Proses autentikasi menjelaskan bahwa pengguna diharuskan memasukan nama pengguna dan kata sandi sebelum mengakses informasi yang ingin didapatkan, apabila nama pengguna dan kata sandi terdaftar, maka pengguna akan diarahkan pada menu pengguna dan diizinkan mengakses informasi yang dibutuhkan. Namun apabila nama pengguna dan kata sandi yang pengguna masukkan tidak terdaftar, maka pesan *invalid* akan muncul dan pengguna akan kembali diarahkan untuk memasukan nama pengguna dan kata sandi yang sesuai atau terdaftar di basis data.

5. KESIMPULAN DAN SARAN

Dari hasil analisis pada penelitian ini, maka dapat disimpulkan analisis penerapan aspek keamanan CIA Triad pada SiakadCloud, yaitu *Confidentiality* yang befokus pada *block direct*, kemudian *Integrity* pada filter data pengguna dan *Availability*, pada autentikasi nya, menunjukkan bahwa sistem berjalan sesuai dengan rancangan. Selanjutnya diharapkan dapat dilakukan analisa terkait keamanan informasi pada sistem dengan menggunakan metode *System Quality Requirements Engineering* (SQUARE) ataupun metode *Failure Mode & Effect Analysis* (FMEA).

6. DAFTAR PUSTAKA

Harahap, A. H., Difa Andani, C., Christie, A., Nurhaliza, D., & Fauzi, A. (2023). Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder. *Jurnal Manajemen Dan Pemasaran Digital*, *1*(2), 73–83.

Miati, L., & Setiawan, R. (2022). Pengaruh E-Service Quality (Siakad Cloud) Terhadap Kepuasan Mahasiswa Stia Yppt Priatim Tasikmalaya. *Jurnal Manajemen Universitas Bung Hatta*, *17*(1), 33–42. https://doi.org/10.37301/jmubh.v17i1.19979

Puriwigati, A. N. (2020). *Sistem Informasi Manajemen-Keamanan Informasi*. *May*.

Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security Fourth Edition. *Learning*, 269, 289.

Wijatmoko, T. E. (2020). Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Pada Kantor Wilayah Kementerian Hukum Dan Ham Diy. *Cyber Security Dan Forensik Digital*, *3*(1), 1–6. https://doi.org/10.14421/csecurity.2020.3.1.1951