Analysis of the Application of CIA Triad Information Security Aspects in Academic Information Systems

Nurmi Hidayasari[1,a)], Kasmawi[2,b)], Mansur[3,c)], M. Iqbal Husaini[4),d)], Putri Nuranisa[5),e)]

[1,2,3,4,5] *Jurusan Teknik Informatika, Politeknik Negeri Bengkalis, Bengkalis, Indonesia*

[a)]nurmihidayasari@polbeng.ac.id
[b)]kasmawi@polbeng.ac.id
[c)]mansur@polbeng.ac.id
[d)]dovikaloo262@gmail.com
[e)]putrinuranisaaa044@gmail.com

Abstract. Threats that often attack information systems such as data leakage, credentials (account compromise), phishing, web-based attacks, malware attacks, cracking (piracy), carding (illegal transactions) and so on. 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, Confidentiality, Integrity, Availability

INTRODUCTION

Information security is all guidelines, rules, best practices, practices to protect the confidentiality, availability and integrity of data and prevent unauthorized access, use, modification, recording and disclosure of information. In fact, information security can not only be applied to IT, but companies/organizations must have an understanding so that when a problem arises, the company/organization can quickly and appropriately handle it. Thus, the need for information security can be met through comprehensive management in every aspect of the company/organization.

A good understanding of information security, as well as proper implementation and in accordance with applicable standards and regulations, then the company/organization can minimize the emergence of system problems or risks better, faster and appropriately. In implementing Information Security, companies/organizations must pay attention to 3 aspects, namely Confidentiality, Integrity, and Availability (CIA)[1]. In general, when attacks, problems, risks that threaten information security arise, then at least one of the CIA aspects will be the target of the attack.

Other sources state that the security aspect of information systems encompasses 4 aspects. Grafinkel stated that computer security encompasses 4 aspects, namely privacy, integrity, authentication and availability. In addition to the four things above, there are still two other aspects that are also often discussed in relation to electronic commerce, namely access control and non-repudiation. Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 4 of 2016 concerning the Information Security Management System, Clause 1 Point 6 is, "Information Security is maintaining the confidentiality, integrity, and availability of information."[2]

Information security is an effort and the right step to protect information assets from potential threats. And indirectly ensures business continuity, reduces emerging risks, and allows for optimizing return on investment. The CIA Triad in information and data systems is very important as a guideline or framework basis, because it contains indicators in preventing Cyber Crime that can harm organizations or companies and is the basis for security programs developed. These three elements are interconnected links in the concept of information protection[3].

Securing information systems can generally be categorized into two types, prevention and handling or repair. Prevention efforts are made so that the information system does not have security gaps, while repair efforts are made if security gaps are exploited. Security can be done from several different screens. For example, the transport screen can use Secure Socket Layer (SSL). Physically, it can also be protected by using a firewall that protects the system with an internet network. The web-based Academic Information System (SIAKAD CLOUD) aims to make it easier for all elements on campus, both lecturers and students, to get the information they need, such as the schedule for carrying out lectures or the Mid-Semester Exam (UTS) and Final Semester Exam (UAS) schedules and all other campus information[4].

Politeknik Negeri Bengkalis as one of the State Vocational Colleges in Indonesia has used 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 confirmed to what extent its security is. It is also necessary to know whether in its implementation SiakadCloud has implemented basic security standards in accordance with CIA Triad. Therefore, this study will analyze the application of CIA Triad information security aspects to measure the extent of security owned by SiakadCloud Politeknik Negeri Bengkalis (Polbeng).

This study focuses on analyzing CIA Triad security aspects on SIAKADCloud Polbeng. CIA Triad aspects consist of Confidentiality including Block Direct, namely the verification of username and password. Integrity, including data and user filtering, by differentiating user access rights according to the selected level. And Availability which includes authentication, namely the availability of a database obtained to access data. This study was conducted to determine the extent of security owned by SIAKADCloud Polbeng as the main information system of Higher Education, whether it has met the information security index standards in accordance with the CIA Triad aspects.

METHODS

The research method used in this study refers to the CIA Triad information security aspect. The stages of work can be seen in Figure 1.

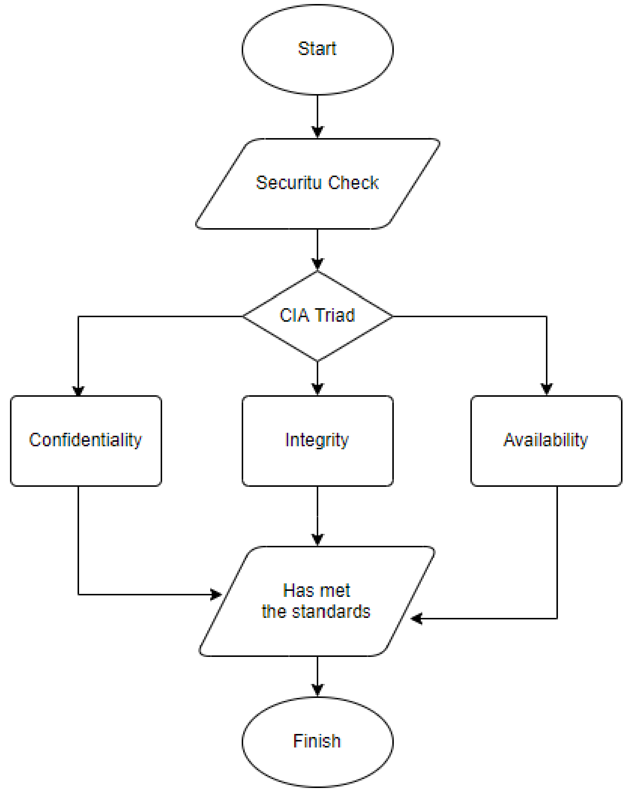
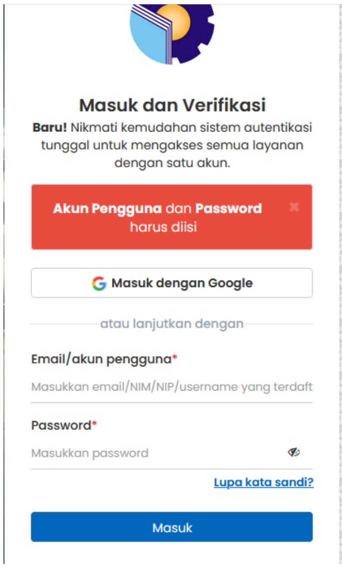


FIGURE 1. The research method

This study uses a qualitative case study research model to determine the application of CIA Triad security aspects on SIAKADCloud. The measurement parameters used are in accordance with CIA Triad standards by conducting direct observations on SIAKADCloud. The research design begins with checking the information security aspects of confidentiality, integrity and finally availability. This study uses observation techniques. The data sources are data used in this study, namely data sourced from references, such as books, scientific articles/papers, reports, surveys and other data sources related to the research being conducted. The data analysis technique used uses qualitative data analysis techniques to analyze the results of the CIA Triad application. These results will be used as a reference to evaluate the system if needed.

RESULTS AND DISCUSSION

1. Confidentiality
   At this stage, Block Direct is performed, where on the login page, the username and password verification will be checked. If the data entered is wrong or empty, what will happen to the system. Then see the contents of the coding and conduct testing on the coding. According to the design, users who try to log into the system must go through a verification page containing the name and password. If the username and password are empty or wrong, a warning will be given, as seen in Figure 2. If the username and password are correct and registered, the user can log in and access the main menu.



Masuk dan Verifikasi

Baru! Nikmati kemudahan sistem autentikasi tunggal untuk mengakses semua layanan dengan satu akun.

Akun Pengguna dan **Password** harus diisi ✖

Masuk dengan Google

atau lanjutkan dengan

Email/akun pengguna*

Masukkan email/NIM/NIP/username yang terdaft

Password*

Masukkan password

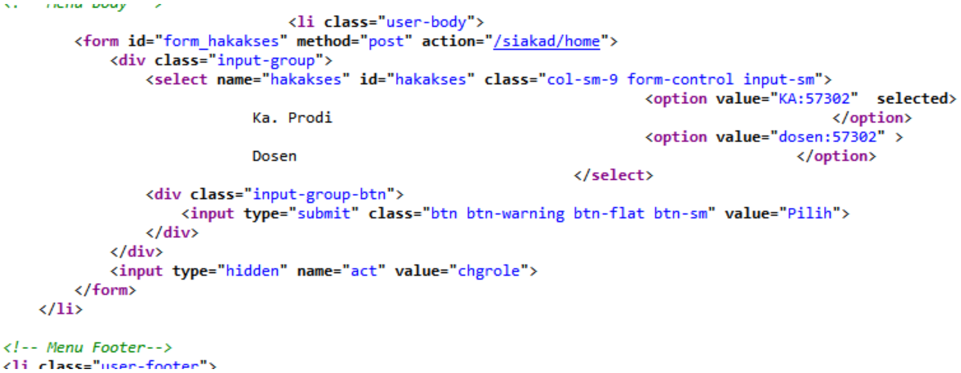
Lupa kata sandi?

Masuk

FIGURE 2. Warning on the system if the input is wrong

2. Integrity

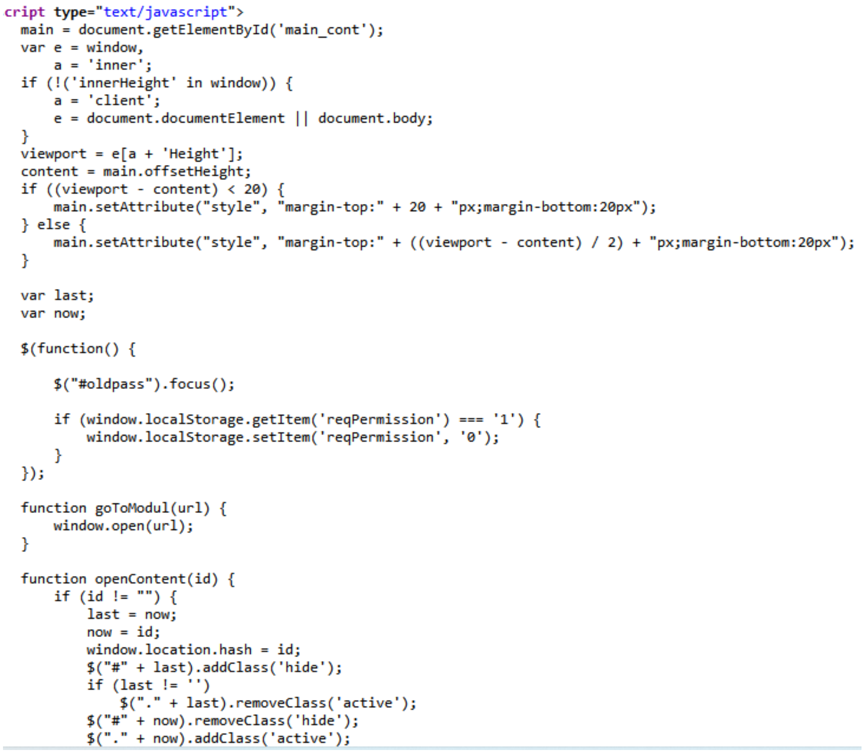
In this aspect, checking User and Data filtering: user level division. For checking, it is required to enter a username, password and select a user level where it aims to differentiate user access according to the selected level, after which the user will be directed to the main menu page according to the specified level and filtered data to prevent data exposure as a whole to unauthorized parties, so that data becomes more protected and data leaks can be reduced and avoided.



```
<!-- Menu Body -->
                                <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">
```

FIGURE 3. Source code for sharing access rights



```
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');
```

FIGURE 4. Data and user filtering source code

The source code used is by using the if branch. Here, if the password entered matches the password registered in the database, then the next system will be run. Where username = username, password = password, and level = level, based on user input, identify whether the program identifies the user as a regular Lecturer or a Lecturer with a Structural Position (such as, Director, Deputy Director, Head of Department, Coordinator. Study Program, etc.). Users as education staff or as students and run the program to retrieve users.

3. Availability
   By performing authentication to see if there is a database obtained to access the data. The authentication process explains that users are required to enter a username and password before accessing the information they want to get, if the username and password are registered, the user will be directed to the user menu and allowed to access the information needed. However, if the username and password entered by the user are not registered, an invalid message will appear and the user will be redirected to enter the appropriate username and password or registered in the database.

CONCLUSIONS

From the results of the analysis in this study, it can be concluded that the analysis of the application of CIA Triad security aspects on SiakadCloud, namely Confidentiality which focuses on direct blocks, then Integrity on user data filters and Availability, on its authentication, shows that the system is running according to design. Furthermore, it is expected that an analysis can be carried out related to information security on the system using the System Quality Requirements Engineering (SQUARE) method or the Failure Mode & Effect Analysis (FMEA) method.

ACKNOWLEDGMENTS

This journal article was written by the author based on the results of Polbeng's PNBP research under the Beginner Lecturer Research scheme funded by Polbeng through the 2024 Research Grant Program and Community Service. The content is entirely the responsibility of the author.

REFERENCES

[1] A. H. Harahap, C. Difa Andani, A. Christie, D. Nurhaliza, and A. Fauzi, “Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder,” *J. Manaj. dan Pemasar. Digit.*, vol. 1, no. 2, pp. 73–83, 2023.

[2] T. E. Wijatmoko, “Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Pada Kantor Wilayah Kementerian Hukum Dan Ham Diy,” *Cyber Secur. dan Forensik Digit.*, vol. 3, no. 1, pp. 1–6, 2020, doi: 10.14421/csecurity.2020.3.1.1951.

[3] A. N. Puriwigati, “Sistem Informasi Manajemen-Keamanan Informasi,” no. May, 2020.

[4] L. Miati and R. Setiawan, “Pengaruh E-Service Quality (Siakad Cloud) Terhadap Kepuasan Mahasiswa Stia Yppt Priatim Tasikmalaya,” *J. Manaj. Univ. Bung Hatta*, vol. 17, no. 1, pp. 33–42, 2022, doi: 10.37301/jmubh.v17i1.19979.