

**KESADARAN KEAMANAN DIGITAL DI ERA *CLOUD COMPUTING* DAN *SMARTPHONE*
PADA SENAT MAHASISWA FAKULTAS SAINS DAN TEKNOLOGI UIN SULTAN THAHA
SAIFUDDIN JAMBI**

Yuyun Ayu Lestari¹, Muhammad Abel Pratama², Al-Fajri³
e-mail: yuyun.ayulestari03@gmail.com¹, abelaja1224@gmail.com²,
alfajriuinjambi@gmail.com³

^{1,2,3}Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, UIN Sultan Thaha
Saifuddin Jambi

ABSTRAK

Perkembangan teknologi *cloud computing* dan *smartphone* sangat membantu meningkatkan efisiensi kinerja organisasi, namun juga hal ini tentunya membawa risiko kejahatan digital yang bisa mengancam keamanan data. Penelitian ini bermaksud untuk menganalisis tingkat kesadaran keamanan digital pada anggota Senat Mahasiswa Fakultas Sains dan Teknologi UIN Sultan Thaha Saifuddin Jambi serta mengukur efektivitas sosialisasi yang dilakukan. Menggunakan metode kualitatif deskriptif melalui observasi, wawancara, dan kuisioner, penelitian melibatkan 20 responden sebagai peserta sosialisasi. Hasil pretest menunjukkan bahwa sebagian besar anggota belum memahami jenis kejahatan digital maupun cara penanggulangannya. Setelah sosialisasi, terjadi peningkatan pemahaman yang signifikan, terutama terkait ancaman digital, penggunaan autentikasi dua faktor (2FA), serta praktik keamanan perangkat dan layanan cloud. Temuan ini menunjukkan bahwa sosialisasi mampu meningkatkan literasi keamanan digital, namun upaya edukasi lanjutan dan penyusunan langkah-langkah penerapan keamanan masih diperlukan agar kesadaran keamanan dapat diterapkan secara konsisten dalam aktivitas organisasi sehari-hari.

Kata Kunci: *cloud computing*, keamanan digital, literasi digital, *smartphone*, sosialisasi.

ABSTRACT

The development of cloud computing and smartphone technology is very helpful in improving the efficiency of organizational performance, but this also brings risks of digital crime that can threaten data security. This research aims to analyze the level of digital security awareness among members of the Student Senate at the Faculty of Science and Technology, UIN Sultan Thaha Saifuddin Jambi, and to measure the effectiveness of the socialization conducted. Using a descriptive qualitative method thru observation, interviews, and questionnaires, the study involved 20 respondents as socialization participants. The pretest results showed that most members did not yet understand the types of digital crime or how to address it. After the socialization, there was a significant increase in understanding, especially regarding digital threats, the use of two-factor authentication (2FA), and device and cloud service security practices. These findings indicate that socialization can improve digital security

Article History

Received: Desember 2025
Reviewed: Desember 2025
Published: Desember 2025

Plagiarism Checker No 784
Prefix DOI : Prefix DOI :
10.8734/Kohesi.v1i2.365
Copyright : Author
Publish by : Kohesi



This work is licensed under
a [Creative Commons
Attribution-
NonCommercial 4.0
International License](https://creativecommons.org/licenses/by-nc/4.0/)



literacy, but further educational efforts and the development of security implementation steps are still needed to ensure security awareness is consistently applied in daily organizational activities.
Keywords: *cloud computing, digital security, digital literacy, smartphones, socialization.*

PENDAHULUAN

Pesatnya perkembangan teknologi informasi saat ini menyebabkan meningkatnya pengiriman data dan informasi secara global. Selain tingginya manfaat yang dirasakan, tingkat risiko dan ancaman penyalahgunaan teknologi informasi juga semakin tinggi dan kompleks. Organisasi menjadi lebih rentan terhadap ancaman atau serangan jaringan atau keamanan informasi yang disebabkan oleh berbagai sumber baik dari aktivitas personal internal atau serangan peretas (Jouini et al., 2014) dalam (Parida Amalia & Muhammad Irwan Padli Nasution, 2024). Keamanan jaringan atau sistem informasi sangat berdampak dengan kehadiran berbagai ancaman atau serangan yang dapat menyebabkan kebocoran informasi sensitif dan rahasia serta penurunan kinerja organisasi (Bustami & Bahri, 2020). Bagi organisasi kemahasiswaan seperti Senat Mahasiswa Fakultas Sains dan Teknologi (SAINTEK) UIN Sultan Thaha Saifuddin Jambi, yang sering menggunakan layanan *cloud* untuk menyimpan dokumen organisasi dan *smartphone* sebagai sarana komunikasi, risiko kebocoran atau penyalahgunaan data dapat berdampak pada kreadibilitas serta efektivitas kegiatan organisasi.

Senat Mahasiswa merupakan salah satu organisasi kemahasiswaan yang didirikan berdasarkan Pedoman Dasar Organisasi Kemahasiswaan yang tercantum dalam Surat Keputusan Mendikbud Nomor 0459/U/1989. Sebagai Badan Perwakilan Mahasiswa tertinggi, Senat Mahasiswa memiliki beberapa tujuan, termasuk meningkatkan kedisiplinan belajar mahasiswa, mendukung dan memastikan keberhasilan pelaksanaan program tri dharma perguruan tinggi, serta membimbing mahasiswa agar perilakunya sesuai dengan norma yang berlaku (Fachrul Rozy Arda et al., 2025). Organisasi Senat Mahasiswa Fakultas Sains dan Teknologi merupakan lembaga legislatif di tingkat fakultas yang didalamnya terdapat perwakilan mahasiswa. Senat mahasiswa (Sema) memiliki tiga fungsi utama, yaitu fungsi legislasi, anggaran, dan pengawasan. Pentingnya keamanan digital bagi organisasi Senat Mahasiswa Fakultas Sains dan Teknologi UIN Sultan Thaha Saifuddin Jambi menjadi perhatian penting bagi semua pihak. Dalam situasi organisasi seperti Senat Mahasiswa Fakultas Sains dan Teknologi UIN Sultan Thaha Saifuddin Jambi, terdapat sejumlah permasalahan dan tantangan yang harus dipertimbangkan dalam konteks keamanan digital pada era *cloud computing* dan *smartphone*:

1. Kurangnya Kesadaran

Salah satu masalah utama adalah kurangnya kesadaran tentang keamanan digital di kalangan anggota organisasi. Banyak anggota organisasi mungkin belum memahami risiko yang mungkin timbul dari pengguna *cloud computing* dan *smartphone*.

2. Keterbatasan Infrastruktur

Infrastruktur jaringan internet pada wilayah sekitar UIN Sultan Thaha Saifuddin Jambi yang tidak stabil dapat meningkatkan kerentanan terhadap serangan.



3. Pelatihan Terbatas

Keterbatasan pelatihan tentang keamanan digital dapat menjadi hambatan. Edukasi kepada anggota organisasi mengenai praktik keamanan digital penting untuk melindungi organisasi dari ancaman potensial.

4. Ketergantungan pada Aplikasi Digital Tanpa Evaluasi

Aplikasi seperti *WhatsApp*, *Instagram*, *Google Drive*, dan aplikasi lainnya sering dipakai namun keamanannya jarang dievaluasi. Anggota organisasi tidak membaca izin aplikasi (*app permissions*) dan tidak ada pengaturan peran atau hak akses.

Berdasarkan temuan-temuan masalah tersebut, secara umum permasalahan yang ditemukan di organisasi Senat Mahasiswa Fakultas Sains dan Teknologi UIN Sultan Thaha Saifuddin Jambi adalah kurangnya kesadaran keamanan digital dalam *era cloud computing* dan *smartphone*. Pencegahan dan penanggulangan terhadap kejahatan siber membutuhkan pendekatan penal dan non penal yang integral dan terpadu. Kebijakan dengan sarana penal adalah upaya penanggulangan kejahatan dengan menggunakan sarana hukum pidana. Sedangkan sarana non penal dapat diartikan sebagai upaya preventif terhadap kejahatan siber, yakni sebagai berikut: Meningkatkan kualitas dan kuantitas aparat penegak hukum yang menguasai teknologi informasi termasuk internet, meningkatkan sarana dan prasarana pendukung bagi penyelidikan dan penyidikan kasus-kasus kejahatan siber, menyusun undang-undang khusus yang mengatur tentang kejahatan siber, dan memberikan edukasi serta literasi yang massif kepada publik terkait kejahatan siber dan bagaimana upaya pencegahannya agar tidak terperangkap dalam modus pelaku kejahatan siber (Umbara & Setiawan, 2022). Kerjasama antara anggota organisasi dan universitas menjadi kunci untuk menghadapi tantangan digital. Langkah-langkah yang diperlukan untuk meminimalisir kemungkinan menjadi korban kejahatan digital antara lain dengan meningkatkan kesadaran adanya kejahatan digital, perbaikan infrastruktur jaringan internet, penyediaan pelatihan tentang keamanan digital, dan selalu melakukan evaluasi mengenai aplikasi digital yang digunakan. *Era cloud computing* dan *smartphone* membawa dampak yang besar, tetapi juga membawa risiko yang perlu dikelola secara bijak.

Dengan melakukan sosialisasi tentang kesadaran keamanan digital di era *cloud computing* dan *smartphone*, anggota organisasi Senat Mahasiswa Fakultas Sains dan Teknologi dapat lebih memahami risiko yang mungkin dihadapi dalam penggunaan teknologi *cloud computing* dan *smartphone*, serta langkah-langkah yang dapat diambil untuk melindungi diri dan aset digital. Edukasi ini penting dilakukan untuk meningkatkan kesadaran dan keamanan digital anggota organisasi, sehingga mereka dapat menggunakan teknologi dengan bijak dan aman. Berdasarkan analisis situasi tersebut, dilakukan kegiatan sosialisasi mengenai keamanan jaringan di era *cloud computing* dan *smartphone* dengan tema “Kesadaran Keamanan Digital di Era *Cloud Computing* dan *Smartphone* Pada Organisasi Senat Mahasiswa Fakultas Sains dan Teknologi UIN Sultan Thaha Saifuddin Jambi”.

Program “Sosialisasi Kesadaran Keamanan Digital di Era *Cloud Computing* dan *Smartphone* Pada Organisasi Senat Mahasiswa Fakultas Sains dan Teknologi UIN Sultan Thaha Saifuddin Jambi” memiliki beberapa tujuan utama yang dirancang untuk melindungi organisasi di tengah transformasi teknologi global. Berikut beberapa tujuan program tersebut:



1. Meningkatkan Kesadaran Keamanan Digital

Salah satu tujuan utama adalah meningkatkan kesadaran anggota organisasi tentang pentingnya keamanan digital. Tujuannya adalah agar mereka memahami risiko yang terkait dengan penggunaan teknologi *cloud computing* dan *smartphone*.

2. Proteksi Data Organisasi

Salah satu tujuan penting adalah melindungi data organisasi. Ini mencakup penerapan regulasi yang memadai dan Langkah-langkah teknis untuk mengamankan data.

3. Kesiapan Menghadapi Ancaman

Membantu anggota organisasi Senat Mahasiswa untuk menjadi lebih siap dalam menghadapi poyensi ancaman siber seperti serangan malware, peretasan dan Upaya phishing.

4. Peningkatan Literasi Teknologi *Cloud* dan *Smartphone*

Menjelaskan cara kerja layanan *cloud*, pengaturan keamanan pada perangkat *smartphone*, serta praktik penggunaan yang aman sehingga anggota tidak hanya sadar risiko, tetapi juga mampu menggunakan teknologi secara benar dan efektif.

5. Penguatan Etika Digital dan Privasi

Menanamkan pemahaman mengenai pentingnya menjaga data pribadi dan organisasi, etika berbagi informasi di platform digital serta dampak dari penyalahgunaan data.

Dengan mencapai tujuan-tujuan ini, program tersebut berusaha untuk menciptakan pemahaman lingkungan digital organisasi yang lebih aman, meningkatkan profesionalitas dan kinerja anggota Senat Mahasiswa, serta mendukung pengembangan kapasitas organisasi dalam era *cloud computing* dan *smartphone*.

METODOLOGI

Metode penelitian berawal dari dasar pemikiran yang membentuk rumusan masalah sehingga membentuk hipotesis awal dengan bantuan dan perspektif penelitian terdahulu. Tujuan akhir dari metode ini adalah untuk menganalisis hasil penelitian (Hafni Sahir, 2021). Penelitian ini menggunakan pendekatan kualitatif deskriptif sebagai metode utama, karena dinilai mampu memberikan gambaran yang mendalam dan menyeluruh mengenai fenomena yang dikaji. Metode kualitatif sering disebut metode penelitian Naturalistik karena penelitiannya dilakukan pada kondisi yang alamiah *Natural Setting* (Sugiyono, 2017) dalam (Permana & Erdansyah, 2022).

Pendekatan ini memungkinkan peneliti untuk menggali pengalaman, persepsi, serta pandangan para aktor yang terlibat langsung dalam proses penerapan teknologi *cloud computing* dan penggunaan *smartphone* di lingkungan organisasi Senat Mahasiswa Fakultas Sains dan Teknologi UIN Sultan Thaha Saifuddin Jambi. Melalui observasi partisipatif, wawancara mendalam, serta penyebaran kuisioner, diharapkan diperoleh informasi yang akurat dan kontekstual mengenai dinamika penerapan kesadaran digital di era *cloud computing* dan *smartphone* ini. Dengan demikian, hasil penelitian tidak hanya bersifat deskriptif, tetapi juga reflektif dan solutif.

Tabel 1. Permasalahan dan Solusi

Permasalahan	Solusi
Ketidakpahaman anggota organisasi SEMA-F SAINTEK UIN Sultan Thaha Saifuddin Jambi mengenai keamanan penggunaan teknologi <i>cloud computing</i> dan <i>smartphone</i> .	1. Memberikan penjelasan mendalam (Presentasi) 2. mempraktikkan cara melakukan keamanan akun dua faktor (2FA) 3. Menampilkan video tutorial keamanan akun <i>cloud</i> dan <i>handphone</i>. 4. Memberikan penjelasan tentang ciri-ciri link phishing.

Lokasi dan Waktu Penelitian

Sosialisasi “Kesadaran Keamanan Digital di Era *Cloud Computing* dan *Smartphone* pada Senat Mahasiswa Fakultas Sains dan Teknologi UIN Sultan Thaha Saifuddin Jambi” dilaksanakan di Gedung Perkuliahan UIN Sultan Thaha Saifuddin Jambi lantai 6. Lokasi ini dipilih karena kesepakatan antara peneliti dan anggota SEMA-F SAINTEK untuk dilaksakannya kegiatan sosialisasi dan dengan dukungan fasilitas yang tersedia dapat mendukung kelancaran proses sosialisasi.

Sosialisasi dilaksanakan pada tanggal 18 September 2025, yang bertepatan dengan periode aktif kegiatan organisasi SEMA-F SAINTEK sehingga memungkinkan peneliti memperoleh data yang relevan dan kontekstual.

Subjek dan Objek Penelitian

Subjek penelitian ini adalah anggota aktif Senat Mahasiswa Fakultas Sains dan Teknologi, yang meliputi pengurus harian, komisi, serta anggota divisi. Jumlah responden yang terlibat adalah 20 orang, dipilih dengan menggunakan teknik *purposive sampling* berdasarkan keterlibatan mereka dalam penggunaan teknologi digital organisasi.

Objek penelitian adalah tingkat kesadaran keamanan digital, termasuk pemahaman mengenai risiko, perilaku penggunaan perangkat, penggunaan layanan *cloud*, serta tindakan preventif dalam menjaga keamanan data organisasi.

HASIL DAN PEMBAHASAN

Pembahasan ini menguraikan hasil temuan penelitian terkait tingkat kesadaran keamanan digital pada anggota Senat Mahasiswa Fakultas Sains dan Teknologi UIN Sultan Thaha Saifuddin Jambi serta efektivitas program sosialisasi dalam meningkatkan pemahaman tersebut. Analisis dilakukan berdasarkan hasil observasi, wawancara, dan kuisioner yang telah kumpulkan dari 20 responden. Untuk mengukur keberhasilan dalam program ini, tim peneliti memilih menggunakan pendekatan pengamatan dengan menyebarkan kuisioner kepada peserta sosialisasi sebelum acara dimulai dan hasilnya terdokumentasi dalam Tabel 2.

Tabel 2. Kuisioner Pemahaman Peserta Sosialisasi

No	Pertanyaan	Pretest		Posttest	
		Sudah	Belum	Sudah	Belum
1	Apakah sebelumnya anda sudah pernah mengikuti sosialisasi ini?	6	14	20	0
2	Apakah anda sudah mengetahui tentang kejahatan digital	13	7	18	2
3	Apakah anda sudah pernah mengalami kejahatan digital?	5	15	5	15
4	Apakah anda sudah mengetahui macam-macam kejahatan digital?	8	12	17	3
5	Apakah anda sudah mengetahui bagaimana cara menanggulangi kejahatan digital?	5	15	16	4

Berdasarkan hasil kuisioner mengenai pemahaman awal peserta terkait sosialisasi kesadaran keamanan digital di era *cloud computing* dan *smartphone*, data menunjukkan bahwa hanya enam dari dua puluh peserta yang pernah mengikuti sosialisasi yang sama, dan sebanyak tujuh orang peserta tidak memiliki pengetahuan dasar tentang kejahatan digital, bahkan terdapat lima belas orang peserta sosialisasi yang tidak mengetahui cara menanggulangi kejahatan digital. Situasi ini menimbulkan minat dan keinginan belajar yang tinggi di kalangan semua peserta yang ikut dalam kegiatan sosialisasi ini.

Peningkatan pemahaman peserta setelah kegiatan sosialisasi dapat terlihat secara jelas melalui perbandingan hasil pretest dan posttest. Pada aspek pemahaman mengenai kejahatan digital, jumlah peserta yang telah mengetahui bentuk-bentuk ancaman meningkat signifikan dari 8 orang pada pretest menjadi 17 orang pada posttest. Hal ini menunjukkan bahwa materi yang disampaikan mampu memberikan pengetahuan baru yang sebelumnya belum dipahami oleh sebagian besar anggota organisasi. Peningkatan ini juga menunjukkan pentingnya edukasi yang bersifat praktis, seperti contoh kasus phishing, malware, dan pencurian identitas digital yang disampaikan dalam sosialisasi.

Selain itu, pada aspek pengetahuan mengenai cara menanggulangi kejahatan digital, terjadi peningkatan pemahaman yang cukup signifikan. Jika sebelumnya hanya 5 orang yang memahami cara pencegahan, setelah sosialisasi meningkat menjadi 16 orang. Edukasi mengenai penggunaan autentikasi dua faktor (2FA), pengelolaan kata sandi, pembaruan perangkat, dan evaluasi izin aplikasi terbukti efektif meningkatkan literasi keamanan peserta. Hal ini relevan dengan temuan pada jurnal (Hilma Harmen et al., 2025) yang menekankan Upaya preventif dalam bentuk edukasi merupakan komponen penting dalam membangun kesadaran keamanan digital di lingkungan organisasi.

Hasil penelitian juga mengindikasikan bahwa masih terdapat sebagian kecil peserta yang belum sepenuhnya memahami ancaman digital meskipun telah mengikuti sosialisasi. Dua peserta masih menunjukkan kurangnya pemahaman mengenai kejahatan digital dan tiga peserta belum memahami secara menyeluruh tipe-tipe ancaman yang ada. Kondisi ini menunjukkan bahwa pembentukan kesadaran keamanan digital tidak dapat dicapai hanya dengan satu kali sosialisasi, namun memerlukan pendekatan



berkelanjutan melalui program pendampingan, pelatihan lanjutan, serta kebijakan keamanan internal organisasi.

Faktor lain yang ditemukan dalam pembahasan adalah rendahnya pengalaman langsung peserta dalam menghadapi kejahatan digital. Berdasarkan data kuisioner, 15 dari 20 peserta belum pernah mengalami insiden siber. Ketidakterpaparan pengalaman ini menjadikan sebagian peserta kurang menyadari tingkat ancaman yang sebenarnya.

Dari sisi penggunaan teknologi, sebagian besar anggota Senat Mahasiswa sangat bergantung pada aplikasi digital seperti Google Drive, WhatsApp, dan berbagai platform media sosial dalam menjalankan aktivitas organisasi. Namun, sebelum sosialisasi dilakukan, mayoritas anggota tidak melakukan evaluasi keamanan aplikasi atau membaca izin akses. Setelah mengikuti sosialisasi, peserta menunjukkan pemahaman yang lebih baik mengenai pentingnya pengaturan privasi, pembatasan akses dokumen, serta penggunaan password yang kuat dan unik. Hal ini merupakan salah satu capaian penting, mengingat kerentanan keamanan sering kali disebabkan oleh kelalaian pengguna, bukan semata kesalahan sistem.

Secara keseluruhan, program sosialisasi terbukti memberikan dampak positif bagi peningkatan kesadaran dan pemahaman keamanan digital di lingkungan Senat Mahasiswa Fakultas Sains dan Teknologi UIN Sultan Thaha Saifuddin Jambi. Meski demikian, temuan penelitian juga menggarisbawahi perlunya penguatan kapasitas digital secara berkelanjutan. Organisasi disarankan untuk menyusun standar operasional prosedur (SOP) keamanan data, melakukan audit keamanan secara berkala, dan menyediakan pelatihan lanjutan untuk memastikan seluruh anggota dapat mengimplementasikan praktik keamanan digital secara konsisten dalam aktivitas organisasi.

KESIMPULAN

Kesadaran keamanan digital di era *cloud computing* dan *smartphone* sangat penting pada saat ini, gempuran teknologi yang semakin canggih dan kejahatan siber dimana-mana membuat kita harus memahami serta mendalami literasi digital terutama hal-hal yang mengenai kewanan digital serta langkah-langkah pencegahannya. Oleh karena itu dalam Penelitian ini menggambarkan tingkat kesadaran keamanan digital anggota Senat Mahasiswa Fakultas Sains dan Teknologi UIN Sultan Thaha Saifuddin Jambi pada awalnya masih rendah, terutama terkait pemahaman ancaman siber dan langkah pencegahannya. Melalui kegiatan sosialisasi yang diberikan, terjadi peningkatan signifikan dalam pengetahuan peserta mengenai jenis kejahatan digital, praktik keamanan pada layanan cloud dan smartphone, serta penggunaan fitur proteksi seperti autentikasi dua faktor (2FA). Meskipun masih terdapat sebagian kecil anggota yang memerlukan pembinaan lanjutan, program sosialisasi ini terbukti efektif dalam meningkatkan literasi keamanan digital. Oleh karena itu, diperlukan edukasi berkelanjutan dan penyusunan SOP keamanan data agar budaya keamanan digital dapat diterapkan secara konsisten di lingkungan organisasi.

DAFTAR PUSTAKA

Bustami, A., & Bahri, S. (2020). Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi : Systematic Review. *Unistek*, 7(2), 59-70. <https://doi.org/10.33592/unistek.v7i2.645>

Fachrul Rozy Arda, Milfa Aisyaroh, Annisatul Padlah, Fauziah Decfina, Olivia Maylina, &



- Sulindawati. (2025). Perancangan Sistem Informasi Pemilihan Ketua Senat Mahasiswa Fakultas (SEMAF) Berbasis Web pada UIN Sumatera Utara. *Jurnal Komputer Teknologi Informasi Dan Sistem Informasi (JUKTISI)*, 3(3), 894-902. <https://doi.org/10.62712/juktisi.v3i3.149>
- Hafni Sahir, S. (2021). *Metodologi Penelitian*. [https://repositori.uma.ac.id/jspui/bitstream/123456789/16455/1/E-Book Metodologi Penelitian Syafri.pdf](https://repositori.uma.ac.id/jspui/bitstream/123456789/16455/1/E-Book%20Metodologi%20Penelitian%20Syafri.pdf)
- Hilma Harmen, Dalimunthe, A. N. S. B. D., Desi Irawan Lestari, Fikri Al Kautsar, Sihombing, J. S., Simanjuntak, T. C. B. S., & Miftahuss'aidah. (2025). Strategi Penguatan Keamanan Informasi Digital dalam Menghadapi Ancaman Siber: Studi Kasus Kementerian Kominfo. *EKOMA : Jurnal Ekonomi, Manajemen, Akuntansi*, 4(6), 8541-8550. <https://doi.org/10.56799/ekoma.v4i6.9870>
- Jouini, M., Rabai, L. B. A., & Aissa, A. Ben. (2014). Classification of security threats in information systems. *Procedia Computer Science*, 32(May), 489-496. <https://doi.org/10.1016/j.procs.2014.05.452>
- Parida Amalia, & Muhammad Irwan Padli Nasution. (2024). Tantangan Terkini Dalam Keamanan Informasi Analisis Resiko Dan Upaya Perlindungan. *Jurnal Ekonomi Bisnis Dan Manajemen*, 2(1), 24-37. <https://doi.org/10.59024/jise.v2i1.529>
- Permana, A. O., & Erdansyah, F. (2022). Analisis Penerapan Prinsip-Prinsip Desain, Tipografi, dan Warna pada Instagram Feed Senat Mahasiswa Universitas Negeri Medan Tahun 2019. *Journal of Education, Humaniora and Social Sciences (JEHSS)*, 5(1), 102-110. <https://doi.org/10.34007/jehss.v5i1.1136>
- Umbara, A., & Setiawan, D. A. (2022). Analisis Kriminologis Terhadap Peningkatan Kejahatan Siber di Masa Pandemi Covid-19. *Jurnal Riset Ilmu Hukum*, 81-88. <https://doi.org/10.29313/jrih.v2i2.1324>