JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 3, Juli 2022, Page 1562-1572
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i3.3999

Implementasi Data Mining dengan Algoritma Naïve Bayes untuk Profiling Korban Penipuan Online di Indonesia

Sunardi[1], Abdul Fadlil[1], Nur Makkie Perdana Kusuma[2,*]

[1] Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2] Program Studi Magister Informatika, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
Email: [1]sunardi@mti.uad.ac.id, [2]fadlil@uad.ac.id, [3]nur2008048034@webmail.uad.ac.id
Email Penulis Korespondensi: nur2008048034@webmail.uad.ac.id

Abstrak−Profiling terhadap korban kejahatan dimaksudkan untuk memudahkan target penyebaran informasi dan melakukan usaha pencegahan. Pembuatan profiling berguna sebagai cara untuk meningkatkan kewaspadaan pengguna internet terhadap *cybercrime*.Penelitian ini bertujuan untuk membuat profiling berdasarkan sosiodemografi korban penipuan *online* melalui Instant Messenger (IM) di Indonesia yang didasarkan pada sosiodemografi korban penipuan secara daring, yaitu usia, jenis kelamin, tingkat pendidikan, domisili, pekerjaan, durasi menggunakan internet dalam sehari, dan media Instant Messenger yang digunakan. Metode yang digunakan dalam penelitian ini adalah metode statistik deskriptif yaitu dengan Data Mining menggunakan metode snowball sampling dengan cara melakukan *sharelink* melalui WhatsApp. Partisipan diberikan tautan untuk mengisi beberapa pertanyaan survey tentang sosiodemografi korban seperti usia, jenis kelamin, pekerjaan, domisili, dan tentang penipuan *online* yang pernah di alami melalui aplikasi IM. Survei dibuat dengan menggunakan GoogleForms dan dikirimkan secara daring melalui WhatsApp kepada partisipan yang pernah menjadi korban penipuan *online*. Teknik Data Mining digunakan untuk menganalisa respon dari 1910 partisipan kemudian diklasifikasikan menggunakan Algoritma Naïve Bayes Hasil penelitian menunjukkan Algoritma Naïve Bayes mempunyai persentase akurasi sebesar 75,28%. Model prediksi terhadap kerentanan korban penipuan *online* adalah responden yang berjenis kelamin perempuan, berusia 27,3 tahun, menggunakan Instagram dan WhatsApp, berdomisili di Provinsi Jawa Tengah, memiliki riwayat pendidikan terakhir hanya sampai dengan SMA, dan menggunakan internet lebih dari delapan jam sehari, serta berstatus sebagai Pelajar/Mahasiswa.

Kata Kunci: Penipuan *Online*; *Phising*; *Profiling*; Korban Kejahatan *Online*; Data Mining

Abstract−Profiling of victims of crime is intended to facilitate the targeting of information dissemination and carry out prevention efforts. Profiling is helpful to increase the awareness of internet users against cybercrime. This study aims to create a sociodemographic profile based on online fraud victims using Instant Messengers in Indonesia based on the sociodemography of online fraud victims, namely age, gender, education level, domicile, occupation, duration of using the internet in a day, and Instant Messenger media used. The method used in this research is the descriptive statistical method, namely Data Mining using the snowball sampling method by sharing a link via WhatsApp. Participants were given a link to fill out several survey questions about the sociodemographic of the victim, such as age, gender, occupation, domicile, and online fraud that had been experienced through the IM application. The survey was created using GoogleForms and sent online via WhatsApp to participants who had been victims of online fraud. The Data Mining technique was used to analyze the responses of 1910 participants and then classified using the Naïve Bayes Algorithm. The results showed that the Naïve Bayes Algorithm has an accuracy percentage of 75.28%. The prediction model for the vulnerability of online fraud victims is a female respondent, aged 27.3 years, using Instagram and WhatsApp, currently living in Central Java Province, education background is high school, and the duration of using the internet more than eight hours a day, and status as a Student/College Student.

Keywords: Online Fraud; Phising; Profiling; Cybercrime Victim; Data Mining

1. PENDAHULUAN

Internet memberikan variasi bermasyarakat yang jauh berbeda dengan kehidupan nyata. Ini yang kemudian disebut dengan dunia maya (*cyber*). Dunia ini merupakan 'tempat' semua orang yang dapat mengakses internet untuk saling berinteraksi satu orang dengan satu lain ataupun satu orang dengan banyak orang, bahkan banyak orang dengan banyak orang sekaligus tanpa harus beranjak posisi. Syaratnya adalah menggunakan perangkat yang terhubung dengan koneksi internet melalui identitas yang disebut akun.

Instant Messenger (IM) adalah salah satu media yang sangat diminati sebagai penghubung antara satu individu kepada individu lain (personal chat), satu individu ke banyak individu lain (*broadcast*), maupun banyak individu sekaligus (*group chat*). IM secara umum terbagi menjadi dua jenis, yaitu *application-based* dan *web based*. *Application-based* diantaranya adalah WhatsApp (WA), Telegram, Skype Messenger, Facebook (Fb) Messenger, dan Direct Message Instagram (IG). *Web-based* diantaranya adalah Meebo, ebuddy, AOL Instant Messenger, Yahoo! Web Messenger, dan Google Talk.

Penggunaan IM dan jejaring sosial saat ini menjadi sebuah kebutuhan dalam hidup sosial bermasyarakat. Dengan munculnya aplikasi IM baik berbasis web maupun aplikasi, orang menjadi semakin mudah dalam berkomunikasi di dalam jaringan maupun antar jaringan, serta memungkinkan pengguna untuk bertukar pesan berupa teks, gambar, suara, video bahkan file dengan instan secara daring hanya melalui melalui perangkat seluler [1]. IM yang sangat sering digunakan saat ini adalah *Social Media Messenger*, yang mempunyai keuntungan yaitu selain bisa digunakan sebagai pertukaran pesan, juga dapat digunakan sebagai media untuk bersosialisasi di dunia maya. Pengguna *Social Media Messenger* dapat berinteraksi dengan orang lain tanpa harus mengunduh aplikasi. Aplikasi yang mempunyai fungsi sebagai IM dan juga media sosial antara lain Facebook, WhatsApp, Instagram, Twitter, dan Telegram.

Submitted: **08/04/2022**; Accepted: **05/07/2022**; Published: **25/07/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 3, Juli 2022, Page 1562-1572
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i3.3999

Dengan adanya internet dan IM maka dunia maya seolah-olah tidak jauh berbeda dengan dunia nyata dalam hal berbagi informasi. Sebagaimana dengan kehidupan bermasyarakat di dunia nyata maka di dunia maya pun juga bermunculan sisi negatif dari manusia sesuai dengan teori Strain[2]: "*crime is a product of society itself*". Di dunia maya, kejahatan yang terjadi dikenal dengan nama cybercrime. Kekhawatiran terhadap tindak kejahatan ini dirasakan di seluruh aspek bidang kehidupan. IM menjadi sebuah dilema dikarenakan akun –akun sosial media messenger tidak menutup kemungkinan adalah akun palsu. Semua orang bisa membuat akun yang tidak sesuai dengan identitas dirinya. Hal ini memungkinkan munculnya celah yang bisa digunakan oleh orang yang tidak bertanggung jawab untuk melakukan kejahatan siber atau penipuan secara daring.

Penipuan secara daring adalah kejahatan yang menggunakan internet untuk keperluan bisnis dan perdagangan sehingga tidak lagi mengandalkan bisnis perusahaan konvensional yang nyata. Penipuan *online* pada prinsipnya sama dengan penipuan konvensional, yang membedakan hanyalah pada sarana perbuatannya yakni menggunakan sistem elektronik (komputer, internet, perangkat telekomunikasi). Penipuan *online* termasuk dalam kelompok kejahatan penyalahgunaan teknologi informasi berupa *Computer Related Fraud*[3], [4].

Reep-van den Bergh & Junger[5] pada tahun 2018 melakukan penelitian di Eropa dengan membuat kategori enam tipe kejahatan siber, yaitu *online shopping fraud*, *online fraud banking/payment*, *other cyber fraud* (*such as advanced fee fraud*), *cyber threats/harassment*, *malware*, dan *hacking*. Penelitian ini menganalisis persentase berdasarkan jumlah korban kejahatan siber yang terjadi di Eropa berdasarkan enam kategori tersebut dalam kurun waktu dari 2009 sampai dengan 2016.

Penggunaan IM seperti Facebook, Twitter, Google+, Instagram, WhatsApp, Telegram, MiChat, dan lain-lain sudah bukan sesuatu yang aneh lagi di Indonesia. Persamaan dari semua IM adalah aplikasi yang populer tersebut membutuhkan akun dengan registrasi berupa akun email dan/atau nomor telepon seluler. Seiring dengan banyaknya serangan dari *cybercriminals* (pelaku *cybercrime*), beberapa perusahaan perangkat lunak terutama pembuat *anti-virus* dan *malware* selalu berusaha untuk menutupi celah dalam sistem yang ada seperti fasilitas verifikasi dua langkah (google mail, yahoo mail, steam *online*, dan lainnya).

Semakin maraknya penggunaan media sosial di internet juga memberikan kesempatan bagi para pelaku kejahatan siber untuk memanfaatkan celah-celah yang ada[6]. Mulai dari kasus penipuan melalui pesan teks ataupun melalui WhatsApp seperti kasus "mama minta pulsa", "anak ditahan polisi karena memiliki narkoba", "ayah kecelakaan", dan masih banyak lagi. Selain menggunakan penipuan melalui pesan, terdapat beberapa kejahatan lain di dunia maya dengan mengirimkan link melalui *direct message* pada media sosial (Instagram atau Facebook) yang dapat membuat penjahat menguasai akun korban. Kejahatan ini melibatkan kegiatan *social engineering* untuk menipu korban[7], [8]. Teknik yang sering digunakan pelaku kejahatan *online* salah satunya adalah *phising*.

Beberapa jenis phishing yang sering ditemukan di dalam kasus penipuan antara lain *spearphising*, manipulasi *link*, *website forgery*, *phone phising*, dan *smishing* [9]–[11]. Di Indonesia *phising* yang sering terjadi adalah *phone phising* dan *smishing*. Pelaku kejahatan sering sekali secara acak menghubungi calon korban melalui telepon, kemudia berpura-pura sebagai karyawan salah satu perusahaan ternama. Pelaku mengimingi calon korban dengan hadiah yang besar, namun calon korban diharuskan untuk melakukan transfer uang kepada rekening tertentu atau diminta untuk memberikan *user* dan *password* aplikasi finansial *online* milik calon korban. Penipuan lain adalah dengan *smishing*, yang mempunyai modus yang sama.

Zulfadhilah et al.[12] di tahun 2016 melakukan penelitian untuk melakukan cyber profiling berdasarkan aktivitas log internet. Penelitian ini menunjukkan bahwa cyber profiling yang dilakukan sangat dipengaruhi oleh faktor lingkungan dan aktivitas sehari-hari. *Profiling* umumnya dilakukan terhadap pelaku kejahatan tetapi *profiling* juga dapat digunakan untuk korban kejahatan. Apabila *profiling* terhadap pelaku kejahatan bertujuan agar memudahkan menangkap pelaku, maka *profiling* terhadap korban kejahatan dimaksudkan untuk memudahkan target penyebaran informasi dan melakukan usaha pencegahan[13]. *Profiling* terhadap pelaku kejahatan siber akan membantu pihak yang berwenang mempersempit lingkup pencarian sehingga menjadi lebih fokus untuk mencari di sumber-sumber lain yang tersedia dengan intensif. Teknologi memang merupakan pertahanan utama melawan serangan siber, pemahaman yang lebih baik terhadap aspek-aspek psikologis, kriminologi, dan sosiologis dapat memberikan masukan upaya perlindungan, dan menangkap pelaku kejahatan siber sebelum jarak menjadi semakin jauh[14].

Data mining dapat digunakan untuk menemukan pola dan korelasi yang menarik dalam data, yang kemudian dapat digunakan untuk menghasilkan pengetahuan. Penambangan data baru-baru ini menjadi relevan dalam pariwisata karena potensinya untuk mengungkap pola yang belum ditemukan dalam kumpulan data besar dan, tidak seperti pendekatan statistik lainnya, kemampuannya untuk memeriksa korelasi non-linier dalam data yang dianalisis. Dibandingkan dengan pendekatan statistik lainnya, *data mining* memiliki asumsi yang lebih sedikit tentang kualitas data karena data mungkin tidak lengkap, berisik, berlebihan, dan dinamis[15].

Pola-pola pada data mining ini bisa bersifat statistik; contohnya adalah tingkat pengangguran dapat diturunkan dan diprediksi menggunakan *data mining*. Korelasi juga dapat digunakan dalam ranah pembelajaran mesin. Misalnya, menggunakan penambangan data ke dalam program pembelajaran mesin untuk memprediksi perilaku pelanggan. Data mining juga bisa digunakan untuk membuat *knowledge based system* untuk memprediksi pola *cybercrime* dan juga pembuatan profiling[16].

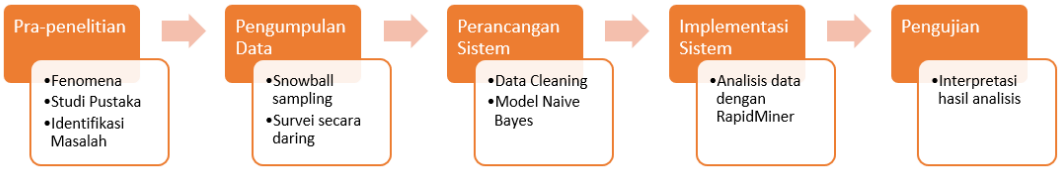
Submitted: **08/04/2022**; Accepted: **05/07/2022**; Published: **25/07/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 3, Juli 2022, Page 1562-1572
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i3.3999

Pembuatan *profiling* ini berguna sebagai cara untuk meningkatkan kewaspadaan pengguna internet terhadap *cybercrime*[17], [18]. Penelitian ini bertujuan untuk membuat *profiling* dengan menggunakan Algortima Naïve Bayes berdasarkan data sosiodemografi korban penipuan *online* melalui IM yang berdampak pada penipuan materi (uang) ataupun pencurian akun IM. Profiling didasarkan pada demografi korban penipuan secara daring, yaitu usia, jenis kelamin, tingkat pendidikan, pekerjaan, durasi penggunaan internet dalam sehari, domisili, dan media IM yang digunakan.

2. METODOLOGI PENELITIAN

Metode yang digunakan dalam penelitian ini adalah metode statistik dengan pendekatan kuantitatif dan Naïve Bayes. Statistik digunakan sebagai alat untuk menyajikan, menggambarkan, atau mengilustrasikan data ke dalam bentuk tabel, gambar, dan diagram sehingga mudah untuk dipahami[19]. Penelitian ini menggunakan juga metode deskriptif dengan cara menggambarkan objek penelitian pada saat keadaan sekarang berdasarkan fakta-fakta sesuai keadaan aslinya berdasarkan hasil survei, kemudian dianalisis dan diinterpretasikan. Sedangkan Model Naïve Bayes digunakan untuk membuat profile terhadap korban kejahatan daring di Indonesia.



Gambar 1. Rancangan penelitian dengan *Modified Waterfall Method*

Tahapan pertama dalam penelitian ini dimulai dengan melakukan pra-penelitian, yaitu dengan mengamati fenomena penipuan secara daring menggunakan IM di Indonesia. Peneliti membuat sebuah dugaan mengenai karakteristik korban kejahatan *online* berdasarkan penelitian yang dilakukan oleh Alzubaidi di Arab Studi [17] tentang karakteristik dari korban kejahatan *online* yaitu sociodemografi korban, perangkat (gawai) yang dimiliki korban, dan aplikasi yang dimiliki korban.

Dalam proses untuk mengumpulkan data, peneltian ini menggunakan teknik snowball sampling. Populasi dalam penelitian ini adalah pengguna IM di Indonesia yang menjadi korban penipuan *online*. Dalam pengumpuan data awal, partisipan dipilih secara acak (*simple random sampling*) yang kemudian dilanjutkan menggunakan teknik snowball sampling dengan memanfaatkan aplikasi WhatsApp dari Bulan Desember 2020 sampai dengan Desember 2021. Partisipan diberikan tautan untuk mengisi beberapa pertanyaan survei melalui Google Form yang berisikan pertanyaan tentang sosiodemografi korban penipuan *online* seperti: nama, nomor telepon, IM, usia, jenis kelamin, pekerjaan, domisili, dan aplikasi Instant Messenger yang digunakan korban. Setelah melakukan pengisian survei, partisipan diminta untuk meneruskan link survei *online* kepada kerabat atau teman menggunakan aplikasi WhatsApp.

Survei terdiri dari dua bagian. Bagian pertama berisikan dengan sociodemografi. Sosiodemografi berasal dari kata *sosio* (sosial) dan demografi yang dapat diartikan sebagai suatu ilmu yang mempelajari segala sesuatu yang berkenaan dengan masyarakat dan proses penduduk di suatu wilayah yang perubahan-perubahan penduduknya dipengaruhi juga oleh proses-proses sosial dan perubahan sosial masyarakat di dalamnya. Karakteristik sosiodemografi antara lain: umur, jenis kelamin, pendidikan, pekerjaan[20]. Bagian kedua berisikan pertanyaan terkait dengan penipuan secara daring seperti jumlah IM yang digunakan, lama penggunaan internet dalam sehari, IM yang digunakan pada saat menjadi korban penipuan secara daring.

Survei dibuat menggunakan GoogleForms untuk memudahkan melakukan pengambilan data secara daring. Penyebaran tautan dilakukan secara acak kepada pengguna media sosial aktif secara *online* dengan menggunakan teknik *Self-Administered Questionnaires*. Teknik *Self-Administered Questionnaires* merupakan metode pengumpulan data dengan formulir terstruktur yang terdiri dari serangkaian pertanyaan tertutup dan pertanyaan terbuka. Selain teknik ini swakelola karena responden mengisinya sendiri (tanpa pewawancara), tetapi juga metode pengumpulan data mencakup wilayah tertentu sehingga memudahkan untuk mengumpulkan data dengan waktu yang relatif lebih singkat. Survei dikirimkan melalui WhatsApp pengguna IM yang ada di Indonesia. Data pribadi milik responden tidak akan dipublikasikan.

Pada tahapan perancangan sistem, data terlebih dahulu dibersihkan sesuai dengan kaidah dalam data mining. RapidMiner difungsikan sebagai tools untuk melakukan pre-processing. Atribut perancangan awal sistem terdiri dari 10 atribut dan 1 label sebagai atribut yang digunakan sebagai prediksi data, yaitu Usia, Jenis Kelamin, Jenjang Pendidikan, Pekerjaan, Durasi menggunakan internet, Domisili, Instant Messenger, Kapan pertama kali menggunakan Instant Messenger, Gawai, Sistem Operasi pada Gawai, dan Label: Pernah menjadi korban penipuan secara daring. Dalam tahapan pre-processing dengan RapidMiner, terdapat beberapa atribut yang mempunyai korelasi rendah. Sebanyak 3 atribut tidak bisa dilanjutkan ke dalam proses analisis dengan model Naïve Bayes sehingga hanya 7 atribut dan 1 label yang bisa diteruskan. Atribut yang digunakan dalam analisis bisa dilihat pada

Submitted: **08/04/2022**; Accepted: **05/07/2022**; Published: **25/07/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 3, Juli 2022, Page 1562-1572
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i3.3999

Tabel 1. Penelitian ini menggunakan algoritma Naïve Bayes sebagai model analisis untuk klasifikasi korban penipuan daring di Indonesia. Algoritma Naïve Bayes selain juga bisa digunakan sebagai metode statistik, mempunyai kemampuan untuk melakukan klasifikasi[16], [21], [22]

Tabel 1. Dataset atribut profile korban kejahatan online

Atribut	Tipe Data	Keterangan
Usia	Integer	Angka
Jenis Kelamin	Binominal	Laki-laki, Perempuan
Jenjang Pendidikan	Polynominal	SMA, D1/D2/D3, D4/S1, S2
Pekerjaan	Polynominal	Pelajar/Mahasiswa, Karyawan Swasta, PNS/ASN, Guru/Pengajar/Instruktur, Wirausaha, Lainnya
Durasi menggunakan internet	Polynominal	Kurang dari 1 jam, 1-3 jam, 4-8 jam, lebih dari 8 jam
Domisili	Polynominal	34 Provinsi di Indonesia
Instant Messenger	Polynominal	Instagram, WhatsApp, Facebook, Telegram, TikTok, Twitter, Line, MiChat, Tinder
Label: Pernah menjadi korban penipuan secara daring	Binominal	Ya, Tidak

Tahapan keempat adalah mengolah data yang sudah melalui tahapan pre-processing ke dalam model klasifikasi dengan Naïve Bayes. RapidMiner menyediakan kemudahan dalam melakukan analisa dalam data mining. Tabel 2 menampilkan sebagian data dari hasil data cleaning pada tahapan preprocessing. Dataset terkumpul sebanyak 1910 data dari responden.

Tabel 2. Dataset sampai dengan 30 responden

No	USIA	Jenis Kelamin	Jenjang Pendidikan	Pekerjaan	Domisili (Provinsi)	Durasi Menggunakan Internet Dalam Sehari	Instant Messenger Yang Biasa Diakses	Apakah Anda Pernah Mengalami Kejahatan Online
1.	19	Perempuan	SMA	Pelajar/Mahasiswa	JAWA BARAT	4 - 8 jam	Instagram, WhatsApp	Tidak
2.	20	Perempuan	SMA	Pelajar/Mahasiswa	JAWA TENGAH	lebih dari 8 jam	Lainnya	Tidak
3.	21	Laki-Laki	D1 / D2 / D3	Pelajar/Mahasiswa	NTB	1 - 3 jam	Telegram	Tidak
4.	20	Laki-Laki	SMA	Pelajar/Mahasiswa	DIY	4 - 8 jam	Line	Tidak
5.	30	Laki-Laki	D4 / S1	Karyawan Swasta	KEPULAUAN RIAU	lebih dari 8 jam	Instagram	Tidak
6.	17	Perempuan	SMA	Pelajar/Mahasiswa	JAWA TENGAH	4 - 8 jam	Instagram	Ya
7.	24	Laki-Laki	D4 / S1	PNS/ASN	PAPUA	1 - 3 jam	Instagram, WhatsApp, Twitter	Ya
8.	33	Laki-Laki	D4 / S1	Karyawan Swasta	JAWA TENGAH	lebih dari 8 jam	Facebook	Ya
9.	21	Perempuan	SMA	Pelajar/Mahasiswa	JAWA TENGAH	1 - 3 jam	Instagram	Ya
10.	19	Perempuan	SMA	Pelajar/Mahasiswa	JAWA BARAT	1 - 3 jam	Instagram	Ya
11.	19	Perempuan	SMA	Pelajar/Mahasiswa	SUMATERA BARAT	lebih dari 8 jam	Instagram, Facebook, Tiktok, WhatsApp, Line, Twitter	Ya
12.	24	Laki-Laki	D1 / D2 / D3	Karyawan Swasta	KEPULAUAN RIAU	1 - 3 jam	Instagram, WhatsApp	Tidak
13.	24	Laki-Laki	D1 / D2 / D3	Pelajar/Mahasiswa	SULAWESI TENGGARA	lebih dari 8 jam	WhatsApp	Tidak
14.	21	Perempuan	D1 / D2 / D3	Pelajar/Mahasiswa	KALIMANTAN TENGAH	kurang dari 1 jam	Instagram	Tidak
15.	29	Perempuan	S2	Guru/Pengajar/ Instruktur	KALIMANTAN SELATAN	kurang dari 1 jam	Instagram, Facebook, Telegram	Tidak
16.	28	Perempuan	D4 / S1	Pelajar/Mahasiswa	JAWA BARAT	1 - 3 jam	Instagram, Tiktok, WhatsApp, Twitter	Tidak
17.	45	Perempuan	D1 / D2 / D3	PNS/ASN	NTB	1 - 3 jam	Instagram, Tiktok, WhatsApp,	Tidak

Submitted: **08/04/2022**; Accepted: **05/07/2022**; Published: **25/07/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 3, Juli 2022, Page 1562-1572
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i3.3999

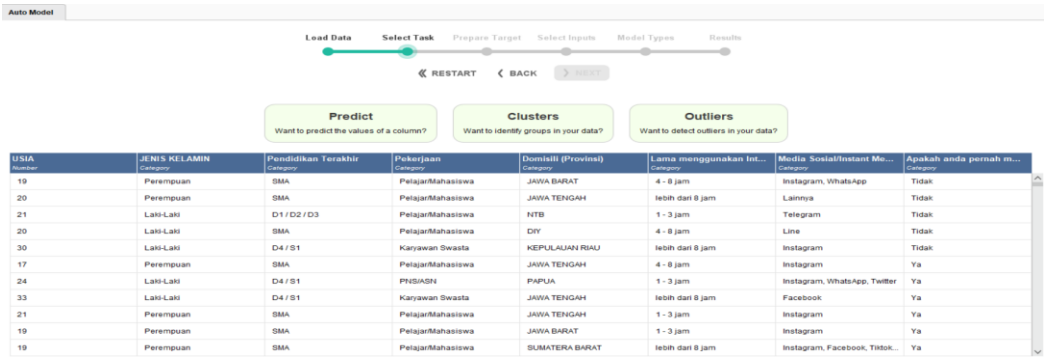
No	USIA	Jenis Kelamin	Jenjang Pendidikan	Pekerjaan	Domisili (Provinsi)	Durasi Menggunakan Internet Dalam Sehari	Instant Messenger Yang Biasa Diakses	Apakah Anda Pernah Mengalami Kejahatan Online
18.	21	Perempuan	SMA	Pelajar/Mahasiswa	JAWA TIMUR	lebih dari 8 jam	Telegram, Twitter Instagram, WhatsApp	Tidak
19.	31	Laki-Laki	S2	Karyawan Swasta	JAWA TIMUR	kurang dari 1 jam	Instagram, Facebook, Tiktok, WhatsApp, Line, Snapchat	Tidak
20.	23	Laki-Laki	D1 / D2 / D3	Karyawan Swasta	KEPULAUAN RIAU	kurang dari 1 jam	Instagram	Tidak
21.	29	Perempuan	S2	Guru/Pengajar/ Instruktur	SUMATERA SELATAN	lebih dari 8 jam	Instagram, Facebook, Tiktok, WhatsApp, Line, Twitter	Ya
22.	23	Perempuan	D1 / D2 / D3	PNS/ASN	SULAWESI SELATAN	kurang dari 1 jam	Instagram, Facebook, Tiktok, WhatsApp, Line, Twitter	Ya
23.	20	Laki-Laki	D1 / D2 / D3	Pelajar/Mahasiswa	NTB	lebih dari 8 jam	Instagram, Facebook, Tiktok, WhatsApp, Line, MiChat	Ya
24.	19	Laki-Laki	SMA	Pelajar/Mahasiswa	KALIMANTAN TENGAH	1 - 3 jam	Instagram, Facebook, Tiktok, WhatsApp, Line, Twitter	Ya
25.	29	Perempuan	SMA	Karyawan Swasta	SULAWESI SELATAN	1 - 3 jam	Instagram, Facebook, Tiktok, WhatsApp, Line, Twitter	Ya
26.	24	Perempuan	D1 / D2 / D3	Pelajar/Mahasiswa	SULAWESI SELATAN	4 - 8 jam	Instagram, Facebook, Tiktok, WhatsApp, Line, Twitter	Ya
27.	34	Perempuan	D4 / S1	Karyawan Swasta	KALIMANTAN TIMUR	1 - 3 jam	Instagram, Facebook, Tiktok, WhatsApp, Line, Twitter	Ya
28.	48	Perempuan	D1 / D2 / D3	PNS/ASN	JAWA TENGAH	4 - 8 jam	Instagram, Facebook, Tiktok, WhatsApp, Line, Twitter	Ya
29.	21	Perempuan	SMA	Pelajar/Mahasiswa	KALIMANTAN BARAT	kurang dari 1 jam	Instagram, Facebook, Tiktok, WhatsApp, Line, Snapchat	Tidak
30.	23	Laki-Laki	D1 / D2 / D3	Karyawan Swasta	JAWA TENGAH	kurang dari 1 jam	Instagram, Facebook, Tiktok, WhatsApp, Line, Twitter	Tidak
…								

Pada tahapan analisis, RapidMiner memberikan kemudahan dengan adanya AutoModel yang secara otomatis melakukan pelatihan data (data training) bersamaan dengan analisis data. Sebanyak 60% dari total data, secara otomatis akan dijadikan sebagai data training. Gambar 2 menampilkan langkah awal dalam melakukan proses analisis dengan RapidMiner. Pada langkah ini, peneliti menggunakan atribut [Apakah Anda Pernah

Submitted: **08/04/2022**; Accepted: **05/07/2022**; Published: **25/07/2022**

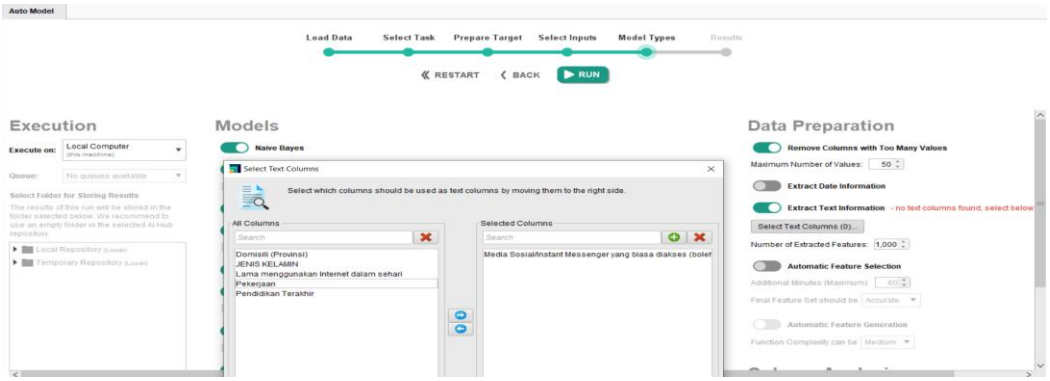
JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 3, Juli 2022, Page 1562-1572
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i3.3999

Mengalami Kejahatan Online] sebagai label untuk melakukan prediksi terhadap atribut-atribut lain yang berkorelasi. Selain melakukan analisis dengan Model Naïve Bayes, RapidMiner juga digunakan melakukan *text mining* untuk atribut Instant Messenger yang digunakan[23]–[25]. Pada Gambar 3, atribut [Instant Messenger Yang Biasa Diakses] digunakan sebagai atribut yang dilakukan *text mining*.



USIA	JENIS KELAMIN	Pendidikan Terakhir	Pekerjaan	Domisili (Provinsi)	Lama menggunakan Int...	Media Sosial/Instant Me...	Apakah anda pernah m...
19	Perempuan	SMA	Pelajar/Mahasiswa	JAWA BARAT	4 - 8 jam	Instagram, WhatsApp	Tidak
20	Perempuan	SMA	Pelajar/Mahasiswa	JAWA TENGAH	lebih dari 8 jam	Lainnya	Tidak
21	Laki-Laki	D1 / D2 / D3	Pelajar/Mahasiswa	NTB	1 - 3 jam	Telegram	Tidak
20	Laki-Laki	SMA	Pelajar/Mahasiswa	DIY	4 - 8 jam	Line	Tidak
30	Laki-Laki	D4 / S1	Karyawan Swasta	KEPULAUAN RIAU	lebih dari 8 jam	Instagram	Tidak
17	Perempuan	SMA	Pelajar/Mahasiswa	JAWA TENGAH	4 - 8 jam	Instagram	Ya
24	Laki-Laki	D4 / S1	PNS/ASN	PAPUA	1 - 3 jam	Instagram, WhatsApp, Twitter	Ya
33	Laki-Laki	D4 / S1	Karyawan Swasta	JAWA TENGAH	lebih dari 8 jam	Facebook	Ya
21	Perempuan	SMA	Pelajar/Mahasiswa	JAWA TENGAH	1 - 3 jam	Instagram	Ya
19	Perempuan	SMA	Pelajar/Mahasiswa	JAWA BARAT	1 - 3 jam	Instagram	Ya
19	Perempuan	SMA	Pelajar/Mahasiswa	SUMATERA BARAT	lebih dari 8 jam	Instagram, Facebook, Tiktok...	Ya

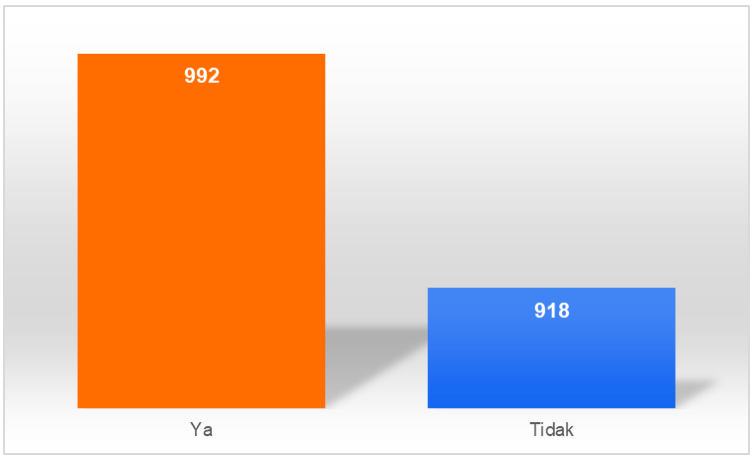
Gambar 2. AutoModel dengan RapidMiner



Gambar 3. Text Mining dengan RapidMiner

3. HASIL DAN PEMBAHASAN

Pada bagian ini dibagi menjadi dua tahapan, yaitu deskripsi data berdasarkan statistik dan hasil analisis data berdasarkan algoritma Naïve Bayes sebagai model pembuatan profil korban kejahatan online. Deskripsi berdasarkan data survey sosiodemografi yang sudah dikumpulkan dari 1910 partisipan pengguna IM. Pada tahapan *preprocessing data mining*, data terlebih dahulu dibersihkan (cleanse) untuk menghilangkan data yang tidak sesuai ataupun data yang hilang (*missing value*). Dari 1910 partisipan yang memberikan respon terhadap survei, didapatkan 992 responden yang pernah menjadi korban penipuan *online* melalui IM, dan 918 tidak pernah menjadi korban penipuan *online* seperti terlihat pada Gambar 1. Deskripsi dibagi dalam kategori usia, jenis kelamin, jenjang pendidikan, pekerjaan, domisili sekarang, durasi menggunakan internet dalam sehari dan media IM yang digunakan. Data kemudian diolah menggunakan Auto Model RapidMiner dan di analisis dengan Algoritma Naïve Bayes dan Text Mining.



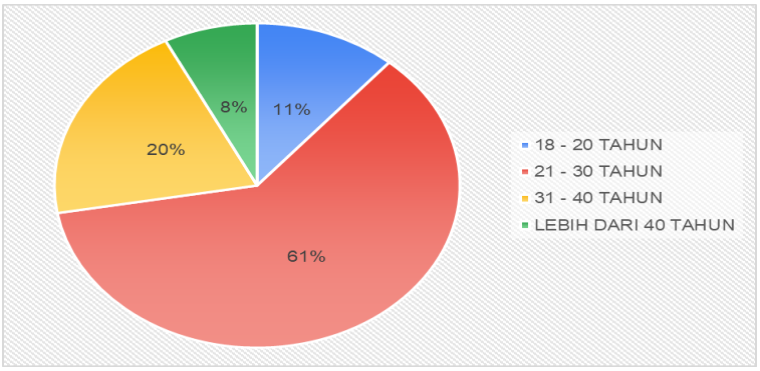
Gambar 4. Perbandingan jumlah partisipan berdasarkan pernah atau tidak menjadi korban penipuan *online*

Submitted: **08/04/2022**; Accepted: **05/07/2022**; Published: **25/07/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 3, Juli 2022, Page 1562-1572
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i3.3999

3.1 Deskripsi Korban Penipuan *Online* Berdasarkan Usia

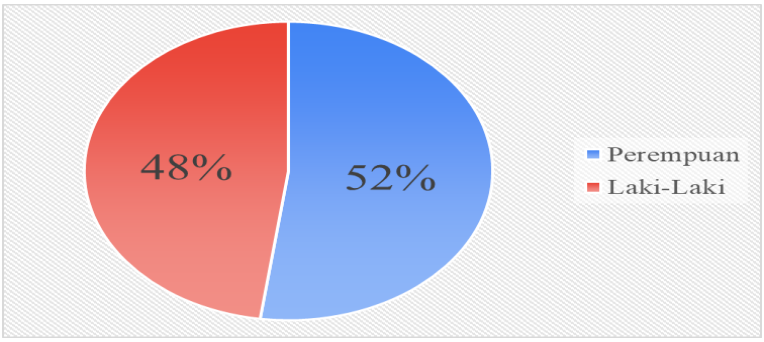
Berdasarkan data dari 992 korban penipuan seperti pada Gambar 5, usia yang paling dominan menjadi korban penipuan *online* berada di rentang 21 sampai dengan 30 tahun sebesar 61% sedangkan yang paling sedikit berada pada rentan usia lebih dari 40 tahun.



Gambar 5. Persentase korban penipuan *online* berdasarkan usia

3.2 Deskripsi Korban Penipuan Online Berdasarkan Jenis Kelamin

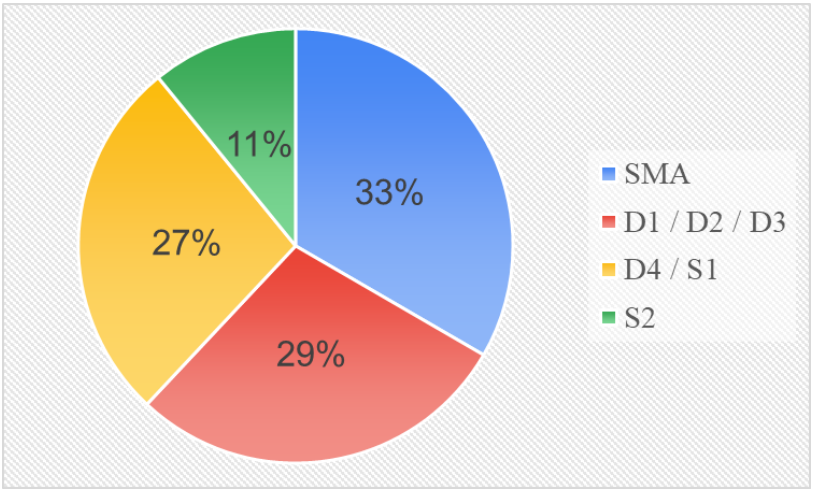
Hasil penelitian menunjukkan bahwa perempuan lebih banyak menjadi korban penipuan *online* daripada laki-laki. Gambar 6 menampilkan dengan jelas tentang pada 992 responden yang menjadi korban penipuan *online* mayoritas adalah perempuan dengan persentase 52%.



Gambar 6. Persentase korban penipuan *online* berdasarkan jenis kelamin

3.3 Deskripsi Korban Penipuan *Online* Berdasarkan Jenjang Pendidikan

Jenjang Pendidikan atau pendidikan terakhir dalam survei ini dibagi menjadi empat pilihan yaitu SMA, Diploma 1/Diploma 2/Diploma, Diploma 4/S1, dan S2. Hasil pada Gambar 7 menunjukkan bahwa dari 992 partisipan yang menjadi korban yang paling sering menjadi korban penipuan *online* adalah responden yang pendidikan terakhirnya SMA dengan presentase 33%.



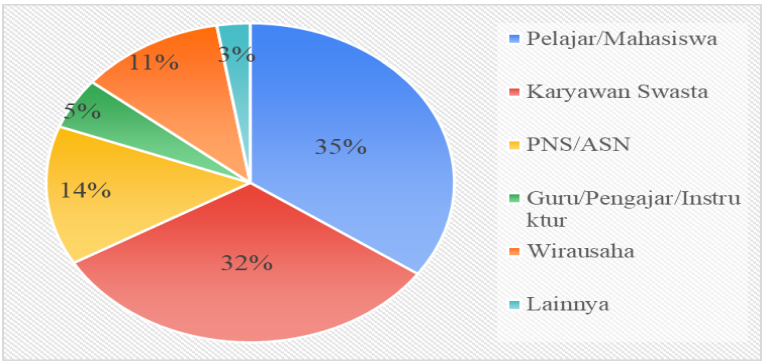
Gambar 7. Persentase korban penipuan *online* berdasarkan jenjang pendidikan

Submitted: **08/04/2022**; Accepted: **05/07/2022**; Published: **25/07/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 3, Juli 2022, Page 1562-1572
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i3.3999

3.4 Deskripsi Korban Penipuan *Online* Berdasarkan Pekerjaan

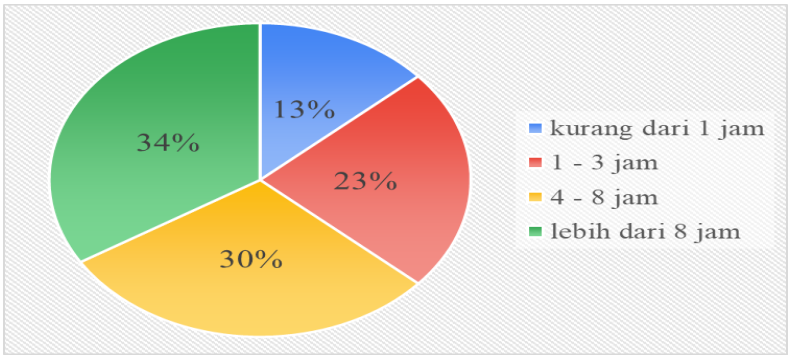
Pekerjaan dalam hal ini dibagi menjadi enam kategori yaitu Pelajar/Mahasiswa, Pegawai Negeri Sipil (PNS), Karyawan Swasta, Guru/Pengajar, Wirausaha, dan Lainnya. Hasil survei dari 992 partisipan yang menjadi korban *online* pada Gambar 8 menunjukkan bahwa yang paling sering menjadi korban penipuan *online* adalah Pelajar/Mahasiswa sebesar 35%.



Gambar 8. Persentase korban penipuan *online* berdasarkan jenis pekerjaan

3.5 Deskripsi Korban Penipuan *Online* Berdasarkan Durasi Menggunakan Internet

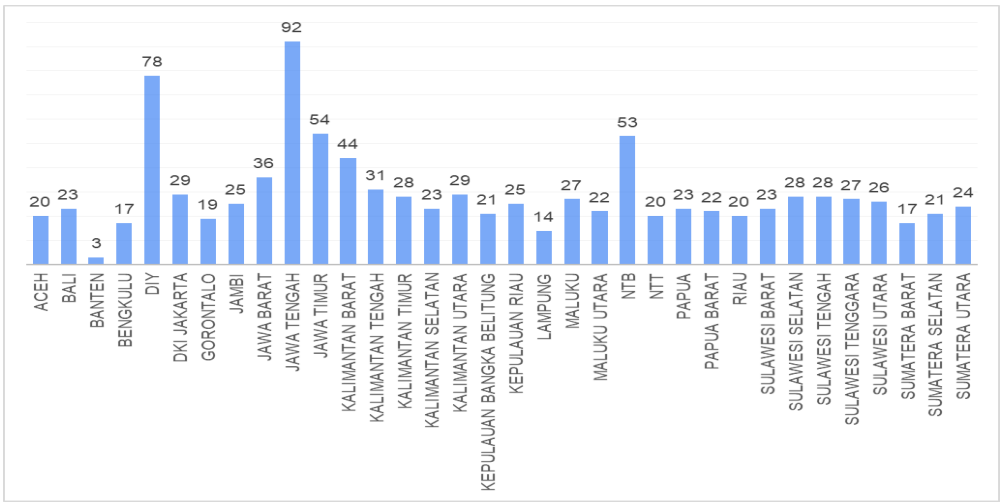
Lama responden menggunakan internet dibuat dalam empat kategori yaitu kurang dari satu jam, satu sampai dengan tiga jam, empat sampai dengan delapan jam, dan lebih dari delapan jam. Hasil pada Gambar 9 menunjukkan bahwa dari 992 partisipan yang menjadi korban *online* yang paling sering menjadi korban penipuan *online* dengan persentase 34% adalah responden yang menggunakan internet lebih dari delapan jam.



Gambar 9. Persentase korban penipuan *online* berdasarkan durasi penggunaan internet

3.6 Deskripsi Korban Penipuan *Online* Berdasarkan Domisili

Domisli responden dikategorikan berdasarkan 34 Provinsi yang ada di Indonesia. Gambar 10 menunjukkan bahwa dari 992 partisipan yang menjadi korban *online* yang paling sering menjadi korban penipuan *online* adalah responden yang berdomisili di Jawa Tengah.



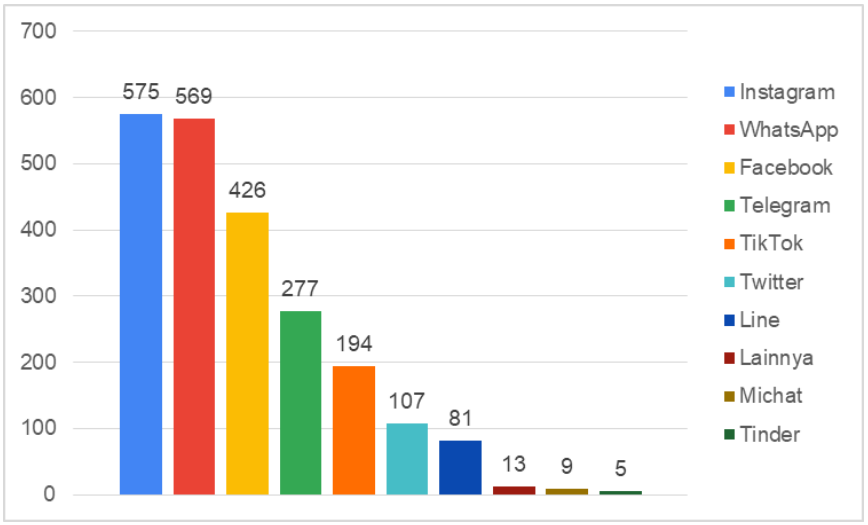
Gambar 10. Persentase korban penipuan *online* berdasarkan domisili

Submitted: **08/04/2022**; Accepted: **05/07/2022**; Published: **25/07/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 3, Juli 2022, Page 1562-1572
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i3.3999

3.7 Deskripsi Media Sosial sering digunakan

Berdasarkan hasil survei terhadap 922 partisipan yang pernah menjadi korban penipuan *online*, setelah dilakukan text mining dengan RapidMiner, maka didapatkan hasil seperti pada Gambar 11. Media sosial yang sering digunakan oleh korban adalah Instagram dan WhatsApp.



Gambar 11. Grafik hasil dari text mining terhadap media sosial yang sering digunakan

3.8 Profiling Korban Penipuan *Online* dengan Algoritma Naïve Bayes

Hasil dari analisis dengan metode Algoritma Naïve Bayes menggunakan RapidMiner memberikan hasil seperti pada Tabel 3. Pada Tabel 3 bisa dilihat bahwa yang mempunyai korelasi paling tinggi terhadap kemungkinan menjadi korban penipuan *online* adalah atribut Usia dengan nilai korelasi 26,1% diikuti oleh Jenis Kelamin dengan korelasi 25,2%. Pembobotan ini memberikan gambaran atribut mana yang paling mempunyai hubungan dengan korban terhadap kemungkinan menjadi korban penipuan *online*.

Tabel 3. Pembobotan berdasarkan Algoritma Naïve Bayes

Attribute	Weight by Correlation (%)
Usia	26,1
Jenis Kelamin	25,2
Instant Messenger	18,9
Domisili	12,3
Pendidikan Terakhir	8,6
Durasi menggunakan internet	4,7
Pekerjaan	4,2

Berdasarkan deskripsi data sosiodemografi tentang korban penipuan *online* pada Gambar 2 sampai dengan 8, yang dikombinasikan dengan pembobotan menggunakan Algoritma Naïve Bayes pada Tabel 3 maka bisa dibuat profile dari korban penipuan *online*. Tabel 4 menunjukkan bahwa yang mempunyai likelihood tinggi sebagai korban penipuan *online* adalah mereka yang berjenis kelamin perempuan, berusia direntang 21 sampai dengan 30 tahun, menggunakan Instagram dan WhatsApp, berdomisili di Provinsi Jawa Tengah, memiliki riwayat pendidikan terakhir hanya sampai dengan SMA, menggunakan internet lebih dari delapan jam sehari, dan berstatus sebagai Pelajar/Mahasiswa.

Tabel 4. Profiling Korban Penipuan *Online* berdasarkan pembobotan Algoritma Naïve Bayes

Atribut	Kemungkinan Tinggi menjadi korban penipuan *online*
Usia	21 – 30 tahun
Jenis Kelamin	Perempuan
Instant Messenger	Instagram, WhatsApp
Domisili	Jawa Tengah
Pendidikan Terakhir	SMA
Durasi menggunakan internet	Lebih dari 8 jam sehari
Pekerjaan	Pelajar/Mahasiswa

Secara spesifik, RapidMiner memberikan gambaran prediksi terhadap kemungkinan seseorang menjadi korban penipuan secara daring seperti pada Tabel 5. Hasil yang ditunjukan Tabel 5 merupakan model simulasi

Submitted: **08/04/2022**; Accepted: **05/07/2022**; Published: **25/07/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 3, Juli 2022, Page 1562-1572
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i3.3999

yang dibuat berdasarkan Algoritma Naïve Bayes. Tabel 4 dan Tabel 5 menunjukkan hasil yang tidak berbeda jauh, kecuali di bagian atribut Usia, dimana pada Tabel 5 menunjukkan hasil yang lebih akurat. Pada Tabel 5, pediksi usia yang mempunyai kemungkinan tinggi sebagai korban penipuan secara daring yaitu pada usia 27,3 tahun.

Tabel 5. Model Simulasi Kemungkinan Korban Penipuan *Online* berdasarkan Algoritma Naïve Bayes

Atribut	Kemungkinan Tinggi menjadi korban penipuan *online*
Usia	27,3 tahun
Jenis Kelamin	Perempuan
Instant Messenger	Instagram, WhatsApp, Facebook
Domisili	Jawa Tengah
Pendidikan Terakhir	SMA
Durasi menggunakan internet	Lebih dari 8 jam sehari
Pekerjaan	Pelajar/Mahasiswa

Tabel 6 menunjukkan hasil dari Confusion Matrix yang bisa digunakan untuk menghitung nilai akurasi, presisi, dan recall. Dapat dilihat pada Tabel 6, terdapat nilai Presisi sebesar 75,28% dan juga nilai Recall sebesar 100%. Hal ini dapat digunakan sebagai cara untuk melihat performa Model Naïve Bayes dalam penelitian ini.

Tabel 6. Confusion Matrix

Kelas	True Tidak	True Ya	Class Precision
Pred. Tidak	0	0	0,00%
Pred. Ya	109	332	75,28%
Class Recall	0,00%	100%	

Performa dari Algoritma dari Naïve Bayes dapat dilihat pada Tabel 7 yang menunjukkan bagaimana implementasi Algoritma Naïve Bayes terhadap pembuatan profil korban penipuan *online* pada penelitian ini. Performa diukur berdasarkan persentase dari Accuracy, Classification Error, Precision dan Recall. Berdasarkan dari Tabel 6 dapat dikatakan bahwa implementasi Naïve Bayes sebagai model pembuatan profil korban penipuan secara daring mempunyai persentase akurasi sebesar 75,28%.

Tabel 7. Analisis Implementasi Algoritma Naïve Bayes

Atribut	Performa (Persentase)
Accuracy	75,28%
Classification Error	24,72%
Precision	75,28%
Recall	100%

4. KESIMPULAN

Berdasakan hasil dan pembahasan, dapat disimpulkan bahwa Algoritma Naïve Bayes dapat digunakan sebagai model dalam pembuatan profil korban kejahatan secara daring dengan persentase akurasi sebesar 75,28%. Model simulasi berdasarkan Algortima Naïve Bayes menunjukkan bahwa yang mempunyai kemungkinan tinggi sebagai korban penipuan *online* adalah mereka yang berjenis kelamin perempuan, berusia 27,3 tahun, sering menggunakan aplikasi Instagram dan WhatsApp, berdomisili di Provinsi Jawa Tengah, dengan jenjang pendidikan terakhir SMA, menggunakan internet lebih dari delapan jam sehari, dan berstatus sebagai Pelajar/Mahasiswa.

REFERENCES

[1] K. O. Oseni, K. Dingley, and P. Hart, "Instant Messaging and Social Networks — The Advantages in Online Research Methodology," *Int. J. Inf. Educ. Technol.*, vol. 8, no. 1, pp. 56–62, 2018, doi: 10.18178/ijiet.2018.8.1.1012.
[2] R. K. Merton, *Social Theory and Social Structure*. New York: The Free Press, 1968.
[3] Ž. Bjelajac, J. Matijašević, and D. Dimitrijević1, "Computer Fraud as a Part of Contemporary Security Challenges," *Rev. Int. Aff.*, vol. LXIII, no. 1147, pp. 5–21, 2012.
[4] S. Schjolberg, "Computer-related offences," *Counc. Eur. Octopus Interface*, no. September, pp. 225–229, 2004, [Online]. Available: http://www.cybercrimelaw.net/documents/Strasbourg.pdf
[5] C. M. M. Reep-van den Bergh and M. Junger, "Victims of cybercrime in Europe: a review of victim surveys," *Crime Sci.*, vol. 7, no. 1, 2018, doi: 10.1186/s40163-018-0079-3.
[6] Study.com, "Role of Instant Messaging in Cybercrime," 2018. https://study.com/academy/lesson/role-of-instant-messaging-in-cybercrime.html
[7] E. Earley, "Understanding social engineering," 2010. https://www.helpnetsecurity.com/2010/03/18/understanding-social-engineering/
[8] N. Y. Conteh and M. D. Royer, "The Unprecedented Rise in Cybercrime and the Role of the Human Vulnerability Factor," pp. 32–43, 2021, doi: 10.4018/978-1-7998-6504-9.ch003.
[9] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Commun. ACM*, vol. 50, pp. 94–100,

Submitted: **08/04/2022**; Accepted: **05/07/2022**; Published: **25/07/2022**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 6, Nomor 3, Juli 2022, Page 1562-1572
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v6i3.3999

2007.
[10] F. Zhou, "Phishing Sites and Prevention Measures," *Int. J. Secur. its Appl.*, pp. 1–10, 2015.
[11] F. Howard and O. Komili, "Poisoned search results : How hackers have automated search engine poisoning attacks to distribute malware .," *Sophos Tech. Pap.*, no. March, pp. 1–15, 2010.
[12] M. Zulfadhilah, Y. Prayudi, and I. Riadi, "Cyber Profiling Using Log Analysis And K-Means Clustering," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 7, 2016, doi: 10.14569/ijacsa.2016.070759.
[13] T. Theodorus M, *Akuntansi Forensik dan Audit Investigatif*. Jakarta: Salemba Empat, 2012.
[14] R. Saroha, "Profiling a Cyber Criminal," *Int. J. Inf. Comput. Technol.*, vol. 4, no. 3, pp. 253–258, 2014.
[15] A. S. Ritonga and I. Muhandhis, "Teknik Data Mining Untuk Mengklasifikasikan Data Ulasan Destinasi Wisata Menggunakan Reduksi Data Principal Component Analysis (Pca)," *Edutic - Sci. J. Informatics Educ.*, vol. 7, no. 2, 2021, doi: 10.21107/edutic.v7i2.9247.
[16] G. Michael, "Knowledge Based System for Predicting Cyber Crime Patterns Using Data Mining," *J. Crit. Rev.*, vol. 7, no. 10, pp. 2043–2053, 2020.
[17] A. Alzubaidi, "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia," *Heliyon*, vol. 7, no. 1, p. e06016, 2021, doi: 10.1016/j.heliyon.2021.e06016.
[18] A. Alzubaidi, "Cybercrime Awareness among Saudi Nationals: Dataset," *Data Br.*, vol. 36, p. 106965, 2021, doi: 10.1016/j.dib.2021.106965.
[19] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Bandung: Alfabeta, 2017.
[20] M. Rita and R. Kusumawati, "PENGARUH VARIABEL SOSIO DEMOGRAFI DAN KARAKTERISTIK FINANSIAL TERHADAP SIKAP, NORMA SUBYEKTIF DAN KONTROL PERILAKU MENGGUNAKAN KARTU KREDIT (Studi Pada Pegawai di UKSW Salatiga)," *J. Manaj. dan Keuang.*, vol. 9, no. 2, pp. 109–128, 2011.
[21] S. Palaniappan, A. Mustapha, C. F. M. Foozy, and R. Atan, "Customer profiling using classification approach for bank telemarketing," *Int. J. Informatics Vis.*, vol. 1, no. 4–2, pp. 214–217, 2017, doi: 10.30630/joiv.1.4-2.68.
[22] H. F. Putro, R. T. Vulandari, and W. L. Y. Saptomo, "Penerapan Metode Naive Bayes Untuk Klasifikasi Pelanggan," *J. Teknol. Inf. dan Komun.*, vol. 8, no. 2, 2020, doi: 10.30646/tikomsin.v8i2.500.
[23] Dr.J.Arunadevi, S.Ramya, and M. R. Raja, "A study of classification algorithms using Rapidminer," *Int. J. Pure Appl. Math.*, vol. Volume 119, no. 12, pp. 15977–15988, 2018.
[24] M. Server, R. Excel, T. Rapidminer, and R.-M. Value, "Analysis of classification algorithms with rapidminer," pp. 517–520.
[25] M. Widyastuti, A. G. Fepdiani Simanjuntak, D. Hartama, A. P. Windarto, and A. Wanto, "Classification Model C.45 on Determining the Quality of Custumer Service in Bank BTN Pematangsiantar Branch," *J. Phys. Conf. Ser.*, vol. 1255, no. 1, 2019, doi: 10.1088/1742-6596/1255/1/012002.

Submitted: **08/04/2022**; Accepted: **05/07/2022**; Published: **25/07/2022**