JURNAL SISFOTENIKA
Vol. 13 No. 2, Juli 2023
p-ISSN: 2087-7897 ; e-ISSN : 2460-5344
DOI : 10.30700/jst.v13i2.1448

Implementasi Naïve Bayes Terhadap Kesadaran Keamanan Informasi Dengan Infeksi Virus Pada Computer

Implementation of Naïve Bayes Against Information Security Awareness with Virus Infections On Computers

Yoyon Arie Budi Suprio[1], Moch. Najib[2]
STIKOM PGRI Banyuwangi, Jl. A.Yani 80 Banyuwangi, Telp. 0333-417902
Teknik Informatika, STIKOM PGRI Banyuwangi
e-mail: 1yoyonstikom@gmail.com, 2jib.stikom@gmail.com,

Abstrak

Dalam perkembanagan teknologi yang semakin maju pesat maka perlu diperhatikan juga mengenai pengamanannya baik itu dari segi software maupun dari sisi datanya maka oleh sebab itu keamanan informasi merupakan pengamanan informasi dari berbagai ancaman agar informasi yang tersimpan dan penting tersebut tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Salah satu ancaman yang dapat mengancam keamanan informasi adalah infeksi virus. Virus meliputi spyware, ransomware, malware dan sebagainya. Oknum tidak bertanggung jawab menggunakan virus untuk mendapatkan informasi penting dari perangkat yang terinfeksi seperti informasi data pribadi serta informasi penting lainnya seperti pada perusahaan atau instansi pemerintah. Di dalam penelitian ini bertujuan untuk mengetahui hubungan antara tingkat kesadaran akan keamanan informasi seseorang dengan besar kemungkinan infeksi virus pada perangkat personal computer menggunakan metode Naïve Bayes. Data diperoleh dari kuesioner yang dibuat secara daring menggunakan Google Form dan dibagikan melalui media sosial. Dari 38 data yang telah terkumpul, sebanyak 29 responden yang perangkat personal computer-nya terinfeksi oleh virus sementara sebanyak 9 responden yang perangkat personal computer-nya tidak terinfeksi oleh virus. Diperoleh bahwa tingkat keamanan informasi sangat berpengaruh pada besar kemungkinan perangkat personal computer seseorang terinfeksi oleh virus. Oleh karena itu kita sebagai pengguna teknologi informasi yang tidak terlepas dari personal komputerharus lebih hati-hati dan selektif dalam menerima informasi dari sumber yang tidak dikenal hal ini dapat menyebabkan terjadinya serangan virus atau malware kedalam perangkat komputer.

Kata kunci*— Keamanan Informasi, Naïve Bayes, Virus*

Abstract

In the development of technology that is advancing rapidly, it is also necessary to pay attention to its security both in terms of software and in terms of data, therefore information security is information security from various threats so that stored and important information is not misused by irresponsible parties. One of the threats that can threaten information security is a virus infection. Viruses include spyware, ransomware, malware and so on. Persons are not responsible for using viruses to obtain important information from infected devices such as

Copyright © 2023 SISFOTENIKA

personal data information and other important information such as companies or government agencies. In this study aims to determine the relationship between the level of awareness of a person's information security with the probability of virus infection on personal computer devices using the Naïve Bayes method. Data was obtained from a questionnaire that was created online using Google Form and shared via social media. From the 38 data collected, 29 respondents had personal computer devices infected with a virus while 9 respondents had personal computer devices not infected with viruses. It was found that the level of information security is very influential on the possibility of a person's personal computer being infected by a virus. Therefore, we as users of information technology that cannot be separated from personal computers must be more careful and selective in receiving information from unknown sources. This can cause virus or malware attacks on computer devices.

Keywords— *Information Security, Naïve Bayes, Virus*

1. PENDAHULUAN

Seiring dengan berkembangnya teknologi informasi dan mudahnya untuk menyimpan atau mendapatkan suatu informasi, tuntutan akan teknologi informasi saat ini semakin diminati. Hal ini dapat dilihat dari penggunaan teknologi informasi yang digunakan saat untuk melakukan aktivitas-aktivitas penting. Salah satu keuntungan dari perkembangan teknologi informasi adalah seseorang dapat dengan lebih mudah berbicara ataupun saling bertukar informasi tanpa adanya batasan wilayah, waktu dan tempat. Perkembangan teknologi informasi yang sangat pesat tersebut berdampak signifikan pada semua lapisan masyarakat. Siapapun dapat dengan mudah memperoleh informasi dari berbagai sumber dengan cepat, akurat, dan murah. Ketika nilai dari sebuah informasi semakin meningkat, demikian juga keinginan seseorang untuk mengakses, memanipulasi dan mengontrol informasi. Namun, tidak dapat dipungkiri jika perkembangan teknologi informasi akan diikuti oleh adanya peningkatan kejahatan siber / cyber crime.[1] Salah satu cyber crime yang dapat mengancam keamanan informasi yaitu penyebaran infeksi virus pada perangkat komputer yang bertujuan untuk mendapatkan suatu informasi penting penggunanya maupun merusak sistem perangkat komputer tersebut.

Di dalam menghadapi pengumpulan informasi secara tidak sah, seseorang ataupun sebuah sistem yang dibuat untuk mencegah tindakan kriminal yang terkait dengan informasi tersebut atau meminimalkan kerusakan yang disebabkan itulah disebut sebagai keamanan informasi. Selain sebuah sistem proteksi informasi yang kuat, manusia juga memainkan peranan penting di dalam implementasi keamanan informasi. Oleh karena itulah, manusia harus berusaha untuk menjaga informasi penting yang dimilikinya dengan baik agar terhindar dari segala bentuk ancaman keamanan informasi. Hal yang dapat dilakukan yaitu dengan meningkatkan kesadaran akan keamanan informasi.

Penelitian ini dilakukan dengan tujuan untuk mengetahui hubungan tingkat kesadaran keamanan informasi seseorang dengan seberapa mungkin perangkat kompter individu tersebut terinfeksi oleh virus yang dapat mengancam keamanan informasi individu tersebut. Pengklasifikasian data dilakukan dengan metode Naïve Bayes. Oleh Suryadi, A., & Harahap, E. (2018) pada sebuah karyanya yaitu Sistem Rekomendasi Penerimaan Mahasiswa Baru Menggunakan Naive Bayes Classifier Di Institut Pendidikan Indonesia. JOUTICA, 3(2), 171–182 tentang Metode Naïve Bayes berguna untuk mengetahui pola data untuk menggali kemungkinan perangkat komputer individu seseorang terinfeksi oleh virus dengan tingkat kesadaran akan keamanan informasi. Dibandingkan dengan metode klasifikasi lainnya, metode klasifikasi Naïve Bayes juga dikatakan memiliki potensi yang baik dalam klasifikasi data berkaitan dengan hal ketepatan dan efisiensi komputasi. Salah satu kelebihan dari metode Naïve

Bayes adalah metode tersebut memerlukan sedikit data latih guna menghitung perkiraan yang dibutuhkan untuk klasifikasi.

Pada penelitian sebelum oleh Syafitri, W pada tahun 2016 dengan metode NIST 800-30 yang merupakan National Institute of Standard and Technology Special Publication (SP) 800-30 ini adalah suatu acuan dalam melakukan manajemen risiko yang diterapkan dalam sistem teknologi informasi yang berstandart pada pemerintah USA, sehingga menurut kami ini cenderung tidak menampilkan tingkat kesadaran dalam keamanan informasi yang lebih akurat yang disertai data-data valid dari para kuisioner.

Kemudian juga ada penelitian sebelumnya yang dilakukan oleh Raden Budiarto pada tahun 2017 yang studi kasusnya pada website Polri halaman 15-17 yang juga menggunakan Metode FMEA dimana ini merupakan sebuah cara untuk merekayasa dalam menetapkan, kemudian identifikasi serta menghapus kegagalan yang telah diketahui. FMEA ini dapat diterapkan selama masa hidup sebuah proses atau layanan masih tetap efektif dan aman, sehingga dalam metode ini masih belum relevan jika diterapkan dalam analisa terhadap suatu keputusan akhir. Pada FMEA ini lebih cocok diterapkan dalam menilai suatu resiko kegagalan atau kesalahan.

Dalam penelitian ini menggunakan Metode Naïve Bayes karena menurut kami metode tersebut sangat cocok dalam pengklasifikasian data data probabilitas digunakan untuk menghitung rentang kemungkinan melalui penambahan gabungan frekuensi, nilai dari sebuah kumpulan data tertentu. Di penelitian ini menggunakan teorema Bayes juga memperikrakan bahwa seluruh variabel adalah independen atau independen satu dengan lainnya, seperti yang diberi dari nilai variabel kelas. Sehingga Metode Naïve Bayes merupakan metode pengelompokkan data dan statistika diusulkan oleh ilmuwan yang bernama Thomas Bayes. Ia menghitung probabilitas waktu yang akan datang berdasarkan pengalaman sebelumnya.

2. METODE PENELITIAN

Metode penelitian dilakukan guna memastikan penyelesaian permasalahan dari penelitian. Pada kasus tersebut menganalisis faktor- faktor pemicu dalam tingkat kesadaran keamanan informasi dengan besar kemungkinan perangkat komputer seseorang terinfeksi oleh virus. Permasalahan- permasalahan tersebut, berikutnya dianalisa dan di hitung untuk menemukan probabilitas permasalahan tersebut.

Penelitian ini menggunakan metode Naive Bayes. Metode Naïve Bayes memiliki tujuan guna menjalankan pengelompokkan data pada sebuah perhitungan, selanjutnya pola itu bisa diterapkan guna memprediksi perhitungan data. Pada metode penelitian ini, menggunakan pengumpulan data informasi dengan mengajukan kuesioner pada responden yang dibuat dengan Google Form dan di bagikan melalui media sosial (Whatsapp). Hasil kuesioner akan di gunakan untuk bahan analisa informasi perhitungan Naïve Bayes.

Dalam pengumpulan data dilakukan dengan menyebar kuisioner dikalangan mahasiswa, dosen, guru, siswa dan karyawan swasta maupun dari instansi pemerintah, dalam proses penyebaran kuisioner ini melibatkan mahasiswa dalam mengirimkan link kuisioner kepada responden melaui media sosial kemudian dikumpulkan dan dianalaisa dari masing-masing hasil kuisioner dari responden. Dari data kuisioner yang disebar melalui media sosial hanya 38 responden yang mengirimkannya kembali atau merespon dari kuisioner yang diberikan.

Tabel 1. Daftar Pertanyaan

Variabel	Pertanyaan	Keterangan
V1	Apakah perangkat komputer Anda	Pertanyaan ini ditujukan untuk

	pernah terinfeksi oleh virus?	responden apakah perangkat komputer responden tersebut pernah terinfeksi virus atau tidak.
K1	Apakah Anda menyebarkan informasi data pribadi Anda seperti E-mail, nomor telepon, password, pin dan sebagainya ke situs web yang tidak Anda ketahui berbahaya atau tidak?	Pada pertanyaan ini bertujuan untuk mengetahui jawaban responden seberapa jauhkah responden menyebarkan data pribadi yang dapat membahayakan data yang bersifat pribadi. Privasi menjadi kekhawatiran seseorang tentang kemungkinan kehilangan privasi sebagai akibat dari penyebaran informasi pribadi kepada pihak ketiga [6].
K2	Apakah Anda pernah mendapatkan e-mail atau sms atau chat yang berisi link atau situs web dari oknum yang tidak Anda kenal?	Pada pertanyaan ini bertujuan untuk mengetahui seberapa maraknya pencurian data pribadi melalui pesan email atau sms yang berisi link atau situs web hingga membahayakan korban yang di tujukan untuk responden. Link yang dibagikan bisa saja mengandung virus / malware yang dapat menginfeksi perangkat seseorang tersebut [6].
K3	Apakah Anda pernah mendownload atau menginstall file/aplikasi tidak resmi/aplikasi crack dari situs yang tidak resmi?	Pada pertanyaan ini bertujuan untuk mengetahui jawaban responden. Sebab bahayanya memasang Aplikasi dari pihak ketiga yang tidak resmi dapat menimbulkan rentan disusupi Malware, adanya ancaman jaringan, smartphone menjadi lemot dan serangan cyber.
K4	Apakah Anda pernah login dengan akun media sosial (Google, Facebook, Twitter, WhatsApp dan sebagainya) ke situs web yang tidak resmi/tidak dikenal?	Kecerobohan dimulai dari ketidak tahuan, hingga dapat menyebabkan kesalahan fatal bagi pengguna. Pada pertanyaan tersebut bertujuan untuk mengukur seberapa banyak responden yang masih mengabaikan data pribadi yang bersifat berbahaya.
K5	Apakah Anda dengan sengaja/tidak sengaja pernah mengunjungi link yang tidak resmi/link yang mencurigakan?	Pada pertanyaan ini di tujukan kepada responden bahayanya mengunjungi situs yang tidak resmi dapat mengakibatkan kebocoran data, jebakan dan penipuan.
K6	Apakah Anda mendownload dan menggunakan aplikasi VPN (Virtual Private Network) ?	Pada pertanyaan tersebut bertujuan untuk mengukur seberapa banyak responden yang masih mengabaikan data pribadi yang bersifat berbahaya. Bahaya menggunakan aplikasi vpn adalah mengancam keamanan perangkat, memperlambat jaringan

internet, bocornya data dan alamat ip

Sebelum melakukan kuisioner kepada responden, penulis telah melakukan beberapa tahapan dalam pengujian validasi pada indikator penilaian pada variabel pertanyaan. Dari variabel tersebut sudah dilakukan survey oleh peneliti tentang apa saja yang bisa menyebabkan sebuah personal komputer terinfeksi virus. Variabel-variabel tersebut yang sering muncul pada aktivitas baik pebulis maupun responden [12].

Naive Bayes Classifier menggunakan pengetahuan statistika menggunakan teori probabilitas. Dimana metode Naïve Bayes ini merupakan metode pengelompokkan yang diambil dari teori kemungkinan dan teorema bayes dalam perkiraan bahwa atribut determinan keputusan dengan sifat bebas atau (independent).

Berikut adalah tahapan perhitungan metode tersebut:

a. Menghitung nilai peluang kasus baru dari setiap hipotesa dengan klas(label) yang ada P(XK|Ci).
b. Menghitung nilai akumulasi peluang dari setiap kelas P(X|Ci).
c. Menghitung nilai P(X|Ci) x P(Ci).
d. Menentukan kelas dari kasus baru tersebut.

Kemudian selanjutnya adalah Langkah-langkah penyelesaian klasifikasi menggunakan rumus metode Naïve Bayes sebagai berikut :

$$P(H|X) = \frac{P(X|H)P(H)}{PX} \qquad (1)$$

Dimana:

X : Sampel Data
H : Hipotesa X adalah data kelas (label)
P(H) : Peluang dari hipotesa H
P(X) : Peluang dari data sampel yang diamati

3. HASIL DAN PEMBAHASAN

Data di dalam tabel berikut adalah data latih yang didapat dari jawaban responden dari kuesioner yang telah dibagikan melalui media sosial. Data yang didapat adalah sebanyak 38 data.

Data tersebut dilakukan terhadap beberapa golongan masyarakat berdasarkan usia dan pekerjaannya. Adapun golongan tersebut adalah dilingkungan akademik yaitu Dosen, mahasiswa serta ada juga yang diluar kampus yaitu guru-guru jenjang SMP dan SMA.

Selain dari pada para akademisi peneliti juga melakukan pada praktisi IT dilingkungan sekitar serta para pegawai di Instansi Pemerintah maupun swasta. Dalam melakukan kuisioner ada beberapa kendala diantaranya adalah kurang pemahan bagi responden tentang bahayanya virus terhadap data sehingga ada diantara mereka yang masih kebingungan.

No	V1	K1	K2	K3	K4	K5	K6
1	Ya	Ya	Ya	Ya	Ya	Ya	Ya
2	Tidak	Ya	Tidak	Ya	Tidak	Ya	Ya
3	Ya	Ya	Ya	Ya	Tidak	Ya	Tidak
4	Ya	Tidak	Ya	Tidak	Tidak	Ya	Tidak
5	Ya	Tidak	Tidak	Ya	Ya	Tidak	Ya
6	Ya	Tidak	Ya	Ya	Ya	Ya	Ya
7	Ya	Tidak	Tidak	Ya	Tidak	Ya	Ya
8	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
9	Tidak	Tidak	Ya	Ya	Tidak	Tidak	Tidak
10	Ya	Ya	Ya	Ya	Ya	Ya	Ya
11	Ya	Tidak	Ya	Ya	Tidak	Tidak	Ya
12	Ya	Tidak	Ya	Ya	Ya	Ya	Ya
13	Ya	Ya	Tidak	Ya	Ya	Ya	Ya
14	Ya	Ya	Ya	Ya	Tidak	Tidak	Tidak
15	Ya	Tidak	Ya	Ya	Ya	Tidak	Ya
16	Ya	Tidak	Ya	Tidak	Tidak	Ya	Ya
17	Ya	Tidak	Tidak	Ya	Tidak	Tidak	Tidak
18	Ya	Tidak	Tidak	Ya	Tidak	Ya	Ya
19	Ya	Tidak	Tidak	Ya	Tidak	Ya	Tidak
20	Ya	Ya	Ya	Ya	Ya	Ya	Tidak
21	Tidak	Ya	Tidak	Tidak	Tidak	Ya	Ya
22	Ya	Ya	Ya	Tidak	Tidak	Tidak	Ya
23	Ya	Tidak	Ya	Ya	Tidak	Tidak	Ya
24	Ya	Ya	Tidak	Ya	Tidak	Tidak	Ya
25	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
26	Ya	Ya	Tidak	Tidak	Tidak	Ya	Ya
27	Tidak	Tidak	Ya	Ya	Ya	Tidak	Ya
28	Ya	Ya	Ya	Tidak	Ya	Tidak	Tidak
29	Ya	Ya	Ya	Tidak	Ya	Ya	Ya
30	Tidak	Ya	Ya	Ya	Tidak	Tidak	Tidak
31	Ya	Tidak	Ya	Ya	Ya	Ya	Tidak
32	Ya	Ya	Ya	Ya	Ya	Ya	Ya
33	Ya	Ya	Tidak	Tidak	Tidak	Ya	Ya
34	Tidak	Ya	Tidak	Ya	Tidak	Tidak	Tidak
35	Ya	Tidak	Ya	Ya	Ya	Tidak	Tidak
36	Ya	Tidak	Tidak	Tidak	Ya	Ya	Tidak
37	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak	Tidak
38	Ya	Ya	Tidak	Tidak	Ya	Ya	Ya

Gambar 1. Hasil Quisioner

Pada gambar 1 diatas menunjukan hasil dari kuisioner terhadap para responden sebanyak 38 Responden yang menginputkan yang terdiri dari berbagai lapisan masyarakat.

Jenis Kelamin	Laki-laki	Perempuan	Total
	26	12	38
	68,40%	31,60%	
Pekerjaan	Sudah Bekerja	Belum Bekerja	Total
	15	23	38
	39,50%	60,50%	
Usia	16-24 tahun	25-50 tahun	Total
	29	9	38
	76,30%	23,70%	

Gambar 2. Data Demografi Responden

Pada gambar 2 merupakan data demografi responden yang telah berpartisipasi dalam kuisioner, dari data tersebut untuk responden laki-laki yang paling banyak dengan usia 16 sampai dengan 24 tahun sekitar 68,4% dengan status pekerjaan belum bekerja yang mencapai 60,5% dari 38 responden.

Kemudian dari hasil quisioner dengan variabel K1 yang menyatakan 28 responden bahwa komputernya pernah terinfeksi virus dan 10 responden belum terinfeksi. Maka dengan data tersebut bahwa serangan virus itu sangat berbahaya dan sebagian besar pernah mengalami.

Dan dari data tersebut menyatakan bahwa para responden 73,6% Komputernya pernah terinfeksi virus.

Kemudian pada variabel K1 didapatkan hasil sekitar 18 responden atau sekitar 47,3% menyatakan bahwa mereka pernah menyebarkan informasi data pribadi mereka seperti email, nomor telepon password pada web yang belum dikenali sebelumnya.

Pada variabel K2 didapatkan hasil yang menyatakan 55,26% atau 21 responden pernah mendapatkan link atau sms dari sumber yang tidak dikenal atau diketahui sebelumnya. Pada K3 bahwa responden yang pernah mendownload atau menginstall aplikasi yang tidak resmi sebanyak 65,78% atau sekitar 25 responden sehingga ini meruapakan salah satu ancaman pada komputer responden.

Selanjutnya pada variabel K4 didapatkan hasil yaitu 16 responden atau 42,1% menyatakan bahwa pernah login dengan sosmed ke situs web yang tidak resmi atau belum dikenali sebelumnya. Kemudian pada K5 yaitu sekitar 21 atau 55,2% responden mengujungi link yang tidak resmi atau belum dikenali sebelumnya atau juga link yang mencurigakan.Sehingga pada hal ini rawan sekali terjadi kebocoran data pribadi responden.

Kemudian yang terakhir pada variabel K6 yang menyatakan bahwa responden yang pernah menggunakan VPN untuk aksen ke web atau terutama web yang diblokir oleh Kementerian Kominfo sebanyak 22 responden atau sekitar 57,8% sehinga ini sangat berbahaya pada responden jika sampai ters menerus menggunakan VPN yaitu terjadinya pengalihan data pribadinya.

Sehingga dengan variabel diatas yang terdiri dari 7 variabel maka kita dapat menganalisa mengenai seberapa besar kesadaran masyarakat terhadap keamanan personal komputernya terhadap virus ataupun terjadinya kebocoran data. Dalam menganalisa dan mengklasifikasikan data tersebut digunakankanlah metode Bayes untuk menentukan hasilnya.

Berikut adalah tabel data testing yang digunakan untuk menentukan hubungan antara tingkat kesadaran keamanan informasi dengan besarnya kemungkinan perangkat komputer terinfeksi oleh virus yang menyerangnya. Data testing yang digunakan adalah sebuah data jika seseorang memiliki kesadaran akan keamanan informasi rendah sehingga setiap pertanyaan memiliki jawaban ‘Ya’.

Tabel 2. Data Testing

K1	K2	K3	K4	K5	K6	V1
Ya	Ya	Ya	Ya	Ya	Ya	?

Setelah menentukan data testing, langkah selanjutnya adalah menghitung P(Ci). P(Ci) pada data latih tersebut ada dua yaitu P(Ci) untuk responden yang terinfeksi oleh virus dan P(Ci) untuk responden yang tidak terinfeksi oleh virus. Jumlah data dalam data latih adalah sebanyak 38 data. Perhitungan P(Ci) data latih tersebut adalah sebagai berikut:

$$P(Terinfeksi\ Virus) = \frac{29}{38} = 0{,}76 \qquad (2)$$

$$P(Tidak\ Terinfeksi\ Virus) = \frac{9}{38} = 0{,}24 \qquad (3)$$

Didapat jumlah responden yang terinfeksi virus adalah sebanyak 29 data sementara yang tidak terinfeksi virus adalah sebanyak 9 data. Berdasarkan perhitungan P(Ci) tersebut didapat bahwa P(Terinfeksi Virus) lebih besar daripada P(Tidak Terinfeksi Virus).

Setelah menghitung P(Ci) langkah selanjutnya yaitu menghitung P(X|Ci). Data perhitungan tersebut adalah sebagai berikut:

Tabel 3. Perhitungan P(X|Ci) Ci = Terinfeksi

P(X|Ci) Ci = Terinfeksi	Kuantitas	Probabilitas
X = K1	14	0,482758621
X = K2	18	0,620689655
X = K3	20	0,689655172
X = K4	15	0,517241379
X = K5	19	0,655172414
X = K6	19	0,655172414

Pada Tabel 3 merupakan Perhitungan P(X|Ci) Ci = Terinfeksi sehingga kami dapat mengetahui datanya terhadap komputer yang terinfeksi.

Tabel 4. Perhitungan P(X|Ci) Ci = Tidak Terinfeksi

P(X|Ci) Ci = Tidak Terinfeksi	Kuantitas	Probabilitas
X = K1	4	0,444444444
X = K2	3	0,333333333
X = K3	5	0,555555556
X = K4	1	0,111111111
X = K5	2	0,222222222
X = K6	3	0,333333333

Pada tabel diatas bertujuan untuk mengetahui perangkat yang dimungkinkan tidak terinfeksi dengan menghitung nilai masing-masing probalitasnya.

Setelah menghitung kedua P(X|Ci) langkah selanjutnya yang dilakukan adalah menentukan nilai kumulatif probabilitas dari setiap kelas P(X|Ci). Perhitungan tersebut dapat dilihat dari dua tabel berikut:

Tabel 5. Perhitungan nilai kumulatif probabilitas setiap kelas P(X|Ci)

P(Xtotal|Terinfeksi)	0,045881859
P(Xtotal|Tidak)	0,000677404

Didapat P(Xtotal|Terinfeksi) serta P(Xtotal|Tidak) dari perhitungan tersebut. Kemudian kedua P(X|Ci) tersebut dikalikan dengan P(Ci) masing-masing kelas untuk menentukan kelas data testing. Tabel di bawah ini menunjukan perhitungan tersebut:

Tabel 6. Perhitungan P(Xtotal|Ci) * P(Ci)

P(Xtotal|Terinfeksi) * P(Terinfeksi)	0,035015103
P(Xtotal|Tidak) * P(Tidak)	0,000160438

Didapat nilai P(Xtotal|Terinfeksi) * P(Terinfeksi) lebih besar daripada P(Xtotal|Tidak) * P(Tidak). Maka data testing tersebut masuk ke dalam kelas terinfeksi. Jadi hasilnya adalah semakin rendah kesadaran keamanan informasi seseorang maka besar kemungkinan perangkat komputer sesoerang tersebut terinfeksi oleh virus.

Dalam hasil kuisioner yang didapat dengan beberapa atribut atau variabel menyatakan bahwa pada atribut di K3 yang paling tinggi hasilnya dengan 25 responden atau 65,8% sering mendownload dan menginstal aplikasi yang sebelumnya belum dimengerti dan 13 responden atau 34,2% menyatakan belum pernah, kemudian atribut berikutnya yang urutan ke dua yaitu pada K5 yang menyatakan mengunjungi link yang tidak resmi atau mencurigakan sebesar 22 responden atau 57,9% dan yang tidak 16 responden 42,1%. Sedangkan atribut lainnya rata-rata 40% yang melakukan aktivitas yang mengarah ke terjadinya serangan virus.

Dengan hasil analisis data kuisioner itu maka berdampak pada kebiasaan responden yang cenderung ceroboh dalam kegiatan yang berkaitan dengan pemanfaatan tekonologi informasi terhadap serangan virus yang menggunakan metode bayes.

Oleh karena itu kami sebagai peneliti selalu memberikan edukasi bagi mereka yang masih awam terhadap keamanan informasi serta dampak-dampaknya jika mengabaikan.

4. KESIMPULAN

Dalam penelitian ini terbukti bahwa tingkat keamanan informasi sangat berpengaruh pada besar kemungkinan perangkat personal computer seseorang terinfeksi oleh virus. Dari 38 data yang telah terkumpul, sebanyak 29 responden yang perangkat personal computer-nya terinfeksi oleh virus sementara sebanyak 9 responen yang perangkat personal computernya tidak terinfeksi oleh virus.

Dari variabel pertanyaan yang paling banyak dilakukan responden yaitu mendownload serta menginstall aplikasi yang belum dimengerti serta mengunjungi link yang sebelumnya belun juga dimengerti sumber link tersebut sehingga ini sebagai pemicu utama perangkat komputer akan terinfeksi oleh virus.

Sehingga apabila seseorang memiliki tingkat kesadaran keamanan informasi rendah, maka semakin besar pula probabilitas perangkat seseorang terinfeksi oleh virus. Hal ini telah dibuktikan dari perhitungan metode Naïve Bayes yang telah dilakukan dalam penelitian tersebut berdasarkan hasil quisioner dan analisa penulis.

Oleh karena itu diharapkan dengan adanya penelitian ini, responen bisa lebih berhati-hati dan meningkatkan tingkat kesadaran akan keamanan informasi data pribadi responden masing-masing agar kecil kemungkinan perangkat personal computer tidak terinfeksi oleh virus maupun malware.

5. SARAN

Penelitian lebih lanjut diharapkan dapat dilakukan dengan responden yang lebih banyak sehingga hasil yang didapatkan dapat lebih efektif dan lebih luas. Selain itu juga metode yang lainnnya dalam pengambilan keputusan atau clustering sehingga diharapkan ada pembanding yang merujuk pada metode mana yang paling tepat. Pertanyaan-pertanyaan di dalam kuesioner juga dapat ditambahkan dengan variabel tambahan lainnya yang berkaitan dengan tingkat kesadaran keamanan informasi agar data dan informasi yang didapat bisa lebih meluas. Perhitungan metode Naïve Bayes juga dapat dilakukan lagi dengan lebih mendetail dan dengan angka probabilitas yang tidak dibulatkan agar didapatkan hasil probabilitas akurat dan tepat.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak-pihak berikut yang telah berkontribusi dan memberikan dukungan agar penelitian ini dapat terlaksana dan terselesaikan dengan baik :

a. STIKOM PGRI Banyuwangi yang telah memberikan dukungan baik finansial maupun non finansial.
b. Segenap teman dosen, mahasiswa, guru dan masyarakat yang telah mengisi dan mengirim jawaban kuesioner yang telah dibagikan melalui media sosial.
c. Saudara Muhammad yang membantu financial secara tidak langsung dalam melakukan kuisioner.
d. Kepada Tim mahasiswa yang tergabung dalam penelitian ini yang tidak dapat kami sebutkan satu persatu.

DAFTAR PUSTAKA

[1] Ting, S. L., Ip, W. H., Tsang, A. H.C. 2011, *International Journal of Software Engineering and Its Applications*. Vol. 5, No.3, Hal 37-46

[2] Syafitri, W., 2016, Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus : Sistem Informasi Akademik Universitas XYZ). 2(2), 8–13.

[3] Budiarto, Raden., 2017,. Penerapan Metode FMEA Untuk Keamanan Sistem Informasi (Studi Kasus : Website POLRI). 15–17.

[4] *Dr. Solomon's Virus Encyclopedia*, 1995 ISBN:1-897661-002.

[5] Anugroho, Prasetyo., 2008, Klasifikasi Email Spam dengan Metode Naïve Bayes Classifier Menggunakan Java Programming.

[6] M. Ridwan, H. Suyono and M. Sarosa, "Penerapan Data Mining untuk Evaluasi Kinerja Akademik Mahasiswa menggunakan Algoritma Naïve Bayes Classifier," EECCIS, vol. VII, 2013

[7] E. Manulu, F. Sianturi and M. Manulu, "Penerapan Algoritma Naïve Bayes untuk Memprediksi Jumlah Produksi Barang Berdasarkan Data Persediaan dan Jumlah Pemesanan PASTRIES," Jurnal Mantik Penusa, vol. I, 2017

[8] H. Muhamad, C. Prasojo, N. Sugianto, L. Surtiningsih and I. Cholissodin, "Optimasi Naïve Bayes Classifier dengan Menggunakan Particle Swarm Optimization pada Data Iris," Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), vol. IV, pp. 180-184, 2017.

[9] C. Fadlan, S. Ningsih and A. Windarto, "Penerapan Metode Naïve Bayes Dalam Klasifikasi Kelayakan Keluarga Penerima Beras Rastra," JUTIM, 2018.

[10] Suryadi, A., & Harahap, E. (2018). Sistem Rekomendasi Penerimaan Mahasiswa Baru Menggunakan Naive Bayes Classifier Di Institut Pendidikan Indonesia. JOUTICA, 3(2), 171–182.

[11] Medkhar, D. S., Bote, M. P., & Deshmukh, S. D. (2013). Heart Disease Prediction System Using Naive Bayes. International Journal Of Enhanced Research In Science Technology & Engineering, 2(3), 1–5. http://doi.org/10.1093/infdis/139.2.232

[12] Akraman, R., Candiwan, C., & Priyadi, Y. (2018). Pengukuran Kesadaran Keamanan Informasi
Dan Privasi Pada Pengguna Smartphone Android Di Indonesia. Jurnal Sistem Informasi Bisnis,
8 (2), 115. https://doi.org/10.21456/vol8iss2pp115-122

[13] Babate, A., Musa, M., Kida, A., & Saidu, M. (2015). State of Cyber Security: Emerging Threats Landscape. International Journal of Advanced Research in Computer Science & Technology, 113 - 119

[14] Jaafar, G. A., Abdullah, S. M., & Ismail, S. (2019). Review of recent detection methods for HTTP DDoS attack. Journal of Computer Networks and Communications, 1-10