

**PENGARUH PENGGUNAAN *INTERNET BANKING* DAN
PERLINDUNGAN NASABAH PENGGUNA FASILITAS *INTERNET
BANKING* TERHADAP *CYBER CRIME* DI DAERAH ISTIMEWA
YOGYAKARTA (DIY)**

SKRIPSI

Diajukan kepada Fakultas Ekonomi Universitas Negeri Yogyakarta
untuk Memenuhi Sebagian Persyaratan guna Memperoleh
Gelar Sarjana Pendidikan



Oleh:
YUSLIA NAILI RAHMAH
14804241008

**PROGRAM STUDI PENDIDIKAN EKONOMI
JURUSAN PENDIDIKAN EKONOMI
FAKULTAS EKONOMI
UNIVERSITAS NEGERI YOGYAKARTA
2018**

PERSETUJUAN

**PENGARUH PENGGUNAAN *INTERNET BANKING* DAN
PERLINDUNGAN NASABAH PENGGUNA FASILITAS *INTERNET
BANKING* TERHADAP *CYBER CRIME* DI DAERAH ISTIMEWA
YOGYAKARTA (DIY)**

SKRIPSI

Oleh:

YUSLIA NAILI RAHMAH
14804241008

Telah disetujui dan disahkan pada tanggal 7 Juni 2018
Untuk dipertahankan di depan Tim Pengaji Skripsi
Program Studi Pendidikan Ekonomi
Fakultas Ekonomi
Universitas Negeri Yogyakarta

Disetujui

Dosen Pembimbing,



Aula Ahmad Hafidh Saiful Fikri, SE.,M.Si.

NIP. 19751028 200501 1 002

PENGESAHAN

Skripsi yang berjudul:

PENGARUH PENGGUNAAN *INTERNET BANKING* DAN PERLINDUNGAN NASABAH PENGGUNA FASILITAS *INTERNET BANKING* TERHADAP *CYBER CRIME* DI DAERAH ISTIMEWA YOGYAKARTA (DIY)

Oleh:

Yuslia Naili Rahmah

14804241008

Telah dipertahankan di depan Dewan Penguji pada tanggal 9 Juli 2018 dan
dinyatakan telah lulus.

Dewan Penguji

Nama	Jabatan	Tanda Tangan	Tanggal
Dr. Maimun Sholeh, M.Si.	Ketua Penguji		18/07/2018
Aula Ahmad H.S.F, SE.,M.Si.	Sekretaris		18/07/2018
Drs. Supriyanto, MM.	Penguji Utama		16/07/2018

Yogyakarta, 19 Juli 2018

Fakultas Ekonomi

Universitas Negeri Yogyakarta

Dekan

Dr. Sugiharsono, M.Si.

NIP. 19550328 198303 1 002

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini:

Nama : Yuslia Naili Rahmah

NIM : 14804241008

Program Studi : Pendidikan Ekonomi

Judul Skripsi : Pengaruh Penggunaan *Internet Banking* dan Perlindungan Nasabah Pengguna Fasilitas *Internet Banking* terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta (DIY)

Menyatakan bahwa skripsi ini merupakan hasil kerja sendiri dan sepanjang pengetahuan saya tidak berisi materi yang dipublikasikan atau dipergunakan persyaratan penyelesaian studi di perguruan tinggi oleh orang lain kecuali pada bagian-bagian tertentu yang saya ambil sebagai acuan atau kutipan dengan mengikuti tata penulisan karya ilmiah yang telah lazim. Apabila terbukti pernyataan ini tidak benar, sepenuhnya menjadi tanggung jawab saya.

Yogyakarta, 7 Juni 2018

Penulis



(Yuslia Naili Rahmah)

NIM. 14804241008

MOTTO

“Sesungguhnya bersama kesulitan ada kemudahan.”

(Q.S Al-Insyirah: 6)

“ Harga kebaikan manusia adalah diukur menurut apa yang telah dilaksanakan atau diperbuatnya.”

(Ali bin Abi Thalib)

“Hidup hanya satu kali, nikmatilah selagi kamu masih bisa menikmatinya dan bersenang-senanglah selagi kamu masih bisa merasakannya.”

(Penulis)

PERSEMBAHAN

Dengan memanjatkan Puji Syukur Kehadirat Allah SWT, Skripsi ini penulis persembahkan kepada:

1. Ayahanda Taufik Hidayat dan Ibunda Jumirah, sebagai sumber semangat bagi penulis yang tak pernah berhenti berdoa.
2. Adiku, Hafidz Khoirul Anam yang selalu mendoakan dan mendukung.
3. Latifah Larassati, Siwi Setiawati, Alifani Mega Pratiwi, dan Siti Nur Bidayah (teman seperjuangan), Khusnul Khotimah dan Ratna Fladira (teman kos), dan teman-teman Pendidikan Ekonomi A 2014 yang selalu memberikan semangat, dukungan, doa, canda, tawa, serta motivasi.

**PENGARUH PENGGUNAAN INTERNET BANKING DAN
PERLINDUNGAN NASABAH PENGGUNA FASILITAS INTERNET
BANKING TERHADAP CYBER CRIME DI DAERAH ISTIMEWA
YOGYAKARTA (DIY)**

Oleh:

Yuslia Naili Rahmah
14804241008

ABSTRAK

Penelitian ini bertujuan untuk mengetahui: (1) pengaruh Penggunaan *Internet Banking* terhadap Terjadinya *Cyber Crime* di wilayah D.I. Yogyakarta, (2) pengaruh Perlindungan Nasabah Bank dalam Penggunaan Fasilitas *Internet Banking* terhadap Terjadinya *Cyber Crime* di wilayah D.I. Yogyakarta, (3) pengaruh Penggunaan *Internet Banking* dan Perlindungan Nasabah Bank dalam Penggunaan Fasilitas *Internet Banking* terhadap Terjadinya *Cyber Crime* di wilayah D.I. Yogyakarta.

Teknik pengumpulan data dilakukan dengan metode pengumpulan data kuisioner. Populasi dalam penelitian ini adalah pengguna fasilitas *internet banking* di wilayah D.I. Yogyakarta. Sampel sebanyak 72 responden yang ditentukan dengan teknik *random sampling*. Uji validitas instrumen menggunakan Korelasi *Product Moment* sedangkan untuk uji reliabilitas menggunakan *Cronbach Alpha*. Teknik analisis yang digunakan adalah analisis regresi linier berganda.

Hasil penelitian menunjukkan bahwa: (1) terdapat pengaruh positif dan signifikan Penggunaan *Internet Banking* terhadap *Cyber Crime* di wilayah DIY dengan nilai koefisien regresi sebesar 0,281 dan nilai signifikansi sebesar 0,037, (2) terdapat pengaruh dari masing-masing variabel Perlindungan Nasabah yaitu terdapat pengaruh negatif dan signifikan *Client Charter* terhadap *Cyber Crime* di wilayah DIY dengan nilai koefisien regresi -0,591 dan nilai signifikansi sebesar 0,022, terdapat pengaruh positif dan signifikan Kerahasiaan Data Nasabah terhadap *Cyber Crime* di wilayah DIY dengan nilai koefisien regresi sebesar 0,630. dan nilai signifikansi sebesar 0,014, tidak terdapat pengaruh dan tidak signifikan *Test and Trial Drive* terhadap *Cyber Crime* di wilayah DIY dengan nilai koefisien regresi sebesar 0,036 dan nilai signifikansi sebesar 0,852, terdapat pengaruh positif dan signifikan *Customer Support Service* terhadap *Cyber Crime* di wilayah DIY dengan nilai koefisien regresi sebesar 0,528 dan nilai signifikansi sebesar 0,014, (3) terdapat pengaruh Penggunaan *Internet Banking* dan Perlindungan Nasabah Pengguna Fasilitas *Internet Banking* (*Client Charter*, Kerahasiaan Data Nasabah, *Test and Trial Drive*, dan *Customer Support Service*) secara bersama-sama terhadap Terjadinya *Cyber Crime* di wilayah DIY dengan nilai *F*_{hitung} sebesar 4,714 dengan nilai signifikansi *F* sebesar 0,001.

Kata Kunci: *Internet Banking, Client Charter, Kerahasiaan Data Nasabah, Test and Trial Drive, Customer Support Service, Cyber Crime*

**THE INFLUENCE OF THE USE OF INTERNET BANKING AND THE
PROTECTION OF USERS OF INTERNET BANKING CLIENTS OF CYBER
CRIME IN THE SPECIAL REGION OF YOGYAKARTA (DIY)**

By:

Yuslia Naili Rahmah
14804241008

ABSTRACT

This research aims to know: (1) the influence of the Internet Banking Usage against the occurrence of Cyber Crime in the special region of Yogyakarta, (2) the influence of Bank Protection in the use of Internet Banking facilities against the occurrence of Cyber Crime in the special region of Yogyakarta, (3) the influence of the use of Internet Banking and Bank Protection in the use of Internet Banking facilities against the occurrence of Cyber Crime in the special region of Yogyakarta.

Data collection technique used in this research is questionnaire. The population in this research is the user of internet banking in the special region of Yogyakarta. The sample are 72 respondents specified with random sampling techniques. Test the validity of the instrument using the correlation of Product Moment and test for reliability using Cronbach Alpha. Analytical techniques used was multiple linear regression analysis.

The results showed that (1) there is a positive influence and significant on the use of Internet Banking against Cyber Crime in an area of DIY with the coefficient regression value of 0,281 and significance value of 0.037, (2) there are the influence of each Customer Protection variable is there is negative influence and significant Client Charter against Cyber Crime in an area of DIY with the coefficient regression value of -0.591 and significance value of 0.022, there is a positive influence and significant on the confidentiality of Customer Data against Cyber Crime in an area of DIY with the coefficient regression value of 0.630 and significance value of 0.014, there was no influence and no significant of Test and Trial Drive against Cyber Crime in an area of DIY with the coefficient regression value of 0.036 and significance value of 0.852, there is a positive influence and significant Customer Support Service against Cyber Crime in an area of DIY with the coefficient regression value of 0.528 and significance value of 0.014, (3) The Influence of the Use of Internet Banking and The Protection of Users of Internet Banking Clients (Client Charter, Confidentiality of Customer Data, Test and Trial Drive, and Customer Support Service) jointly against the occurrence of Cyber Crime in the region of DIY with the value F_{count} with value of 4.714 and F significance of 0.001.

Keyword: Internet Banking, Client Charter, Customer Data Confidentiality, Test and Trial Drive, Customer Support Service, Cyber Crime

KATA PENGANTAR

Puji syukur atas kehadirat Allah SWT yang telah memberikan rahmat serta hidayah-Nya sehingga penyusunan tugas akhir skripsi dengan judul “Pengaruh Penggunaan *Internet Banking* dan Perlindungan Nasabah Pengguna Fasilitas *Internet Banking* terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta” dapat diselesaikan.

Penulis mengucapkan terimakasih atas bantuan dari banyak pihak diantaranya:

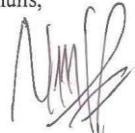
1. Prof. Dr. Sutrisna Wibawa, M.Pd., selaku Rektor Universitas Negeri Yogyakarta yang telah memberikan ilmu dan motivasi selama penulis menempuh studi di perguruan tinggi.
2. Dr. Sugiharsono, M.Si., selaku Dekan Fakultas Ekonomi, Universitas Negeri Yogyakarta yang telah memberikan dukungan dan pengarahan selama masa perkuliahan.
3. Tejo Nurseto, M.Pd., selaku Ketua Jurusan Pendidikan Ekonomi yang memberikan persetujuan Tugas Akhir Skripsi.
4. Dr. Endang Mulyani, M.Si., selaku dosen pembimbing akademik yang telah sabar memberikan arahan dan masukan selama penulis menuntut ilmu.
5. Aula Ahmad Hafidh Saiful Fikri, SE.,M.Si., selaku dosen pembimbing skripsi yang telah memberikan ilmu, waktu, tenaga, dan bimbingannya dalam membimbing dan mengarahkan selama penyusunan skripsi.
6. Drs. Supriyanto, MM., selaku dosen narasumber yang telah sabar memberikan saran dan pengarahan selama penyusunan skripsi.

7. Segenap pengajar dan karyawan Fakultas Ekonomi Universitas Negeri Yogyakarta yang telah memberikan pengajaran, ilmu pengetahuan, dan pengalaman selama penulis menimba ilmu.
8. Teman-teman Pendidikan Ekonomi 2014 yang telah membantu memberikan solusi atas kendala-kendala dalam menyelesaikan penulisan tugas akhir skripsi ini.
9. Semua pihak yang telah membantu baik secara langsung maupun tidak langsung sehingga tugas akhir skripsi ini dapat diselesaikan.

Semoga kebaikan semua pihak dicatat sebagai amalan oleh Allah SWT dan diberikan kemudahan dalam setiap urusannya. Penulis menyadari masih banyak kekurangan dalam penulisan tugas akhir skripsi ini. Oleh karena itu, saran dan kritik yang bersifat membangun sangat penulis harapkan demi penyempurnaan penyusunan tugas akhir skripsi di kemudian hari. Semoga hasil penelitian ini bermanfaat dan dapat dijadikan referensi penelitian bagi peneliti selanjutnya.

Yogyakarta, 5 Juni 2018

Penulis,



Yuslia Naili Rahmah

NIM. 14804241008

DAFTAR ISI

Halaman

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN	iii
PERNYATAAN KEASLIAN SKRIPSI	iv
MOTTO	v
PERSEMBAHAN	vi
ABSTRAK	vii
ABSTRACT	viii
KATA PENGANTAR	ix
DAFTAR ISI	xi
DAFTAR TABEL	xiv
DAFTAR GAMBAR	xv
DAFTAR GRAFIK	xvi
DAFTAR LAMPIRAN	xvii
BAB I. PENDAHULUAN	1
A. Latar Belakang	1
B. Identifikasi Masalah	9
C. Batasan Masalah	10
D. Rumusan Masalah	10
E. Tujuan Penelitian	11
F. Manfaat Penelitian	11
1. Manfaat Teoritis	11
2. Manfaat Praktis	12
BAB II. KAJIAN PUSTAKA	13
A. Kajian Teori	13
1. <i>Cyber Crime</i>	13
a. Pengertian <i>Cyber Crime</i>	13
b. Bentuk Potensi <i>Cyber Crime</i> dalam Kegiatan Perbankan..	15
c. Jenis-jenis <i>Cyber Crime</i>	17
d. Hambatan dalam Penanganan <i>Cyber Crime</i>	20
2. Perbankan	22
a. Pengertian Bank dan Perbankan	22
b. Pengertian Nasabah	23
c. Pengawasan Perbankan	24
3. <i>Internet Banking</i>	25
a. Pengertian <i>Internet Banking</i>	25
b. Tujuan <i>Internet Banking</i>	25
c. Faktor-faktor yang Mempengaruhi Penggunaan <i>Internet Banking</i>	27
d. Produk atau Jasa <i>Internet Banking</i>	29
e. Sistem Keamanan <i>Internet Banking</i>	31
f. Resiko Spesifik untuk <i>Internet Banking</i>	33

g. Prinsip-prinsip dalam Pengaturan <i>Internet Banking</i>	35
h. Perlindungan Nasabah	37
i. Pengaturan <i>Internet Banking</i> di Indonesia	40
B. Penelitian yang Relevan	41
C. Kerangka Berfikir	44
D. Paradigma Penelitian	48
E. Hipotesis Penelitian	49
BAB III. METODE PENELITIAN	50
A. Desain Penelitian	50
B. Tempat dan Waktu Penelitian	50
C. Populasi dan Sampel Penelitian	50
D. Definisi Operasional Variabel	51
E. Teknik dan Instrumen Pengumpulan Data	54
1. Teknik Pengumpulan Data	54
2. Instrumen Pengumpulan Data	55
F. Vaiditas dan Reliabilitas Instrumen	56
1. Uji Validitas	56
2. Uji Reliabilitas	57
G. Teknik Analisis Data	60
1. Analisis Deskriptif	60
2. Uji Prasyarat Analisis	62
a. Uji Linearitas	62
b. Multikoleniaritas	62
c. Heteroskedastisitas	63
d. Uji Normalitas	63
3. Regresi Linier Berganda	64
4. Uji Kelayakan Model	65
a. Koefisien Determinasi	65
b. Uji F	65
c. Uji t	66
5. Mencari Sumbangan Relatif dan Sumbangan Efektif	66
a. Sumbangan Relatif	66
b. Sumbangan Efektif	67
BAB IV. HASIL PENELITIAN DAN PEMBAHASAN	68
A. Hasil Penelitian	68
1. Deskripsi Data	68
2. Deskripsi Variabel Penelitian	72
3. Uji Prasyarat Analisis Data	82
4. Uji Hipotesis	84
B. Pembahasan Hasil Penelitian	90
C. Keterbatasan Penelitian	100
BAB V. SIMPULAN DAN SARAN	102
A. Simpulan	102
B. Implikasi	104
C. Saran	106
DAFTAR PUSTAKA	109

LAMPIRAN	112
----------------	-----

DAFTAR TABEL

Tabel	Halaman
1. Top 20 Negara Pengguna <i>Internet</i> Tertinggi	2
2. Kisi-kisi Kuesioner	55
3. Hasil Uji Validitas	58
4. Tingkatan Hasil Estimasi Reliabilitas	59
5. Hasil Uji Reliabilitas	59
6. Demografi Responden Berdasarkan Jenis Kelamin.....	68
7. Demografi Responden Berdasarkan Usia	69
8. Demografi Responden Berdasarkan Lama Penggunaan <i>Internet Banking</i>	70
9. Demografi Responden Berdasarkan Intensitas Penggunaan <i>Internet Banking</i> per Bulan	71
10. Distribusi Frekuensi Variabel Cyber Crime	72
11. Distribusi Kecenderungan Variabel Cyber Crime	73
12. Distribusi Frekuensi Variabel Penggunaan Internet Banking	74
13. Distribusi Kecenderungan Variabel Penggunaan Internet Banking	75
14. Distribusi Frekuensi Variabel Client Charter	76
15. Distribusi Kecenderungan Variabel Client Charter	77
16. Distribusi Frekuensi Variabel Kerahasiaan Data Nasabah	78
17. Distribusi Kecenderungan Variabel Client Charter	78
18. Distribusi Frekuensi Variabel Test and Trial Drive	79
19. Distribusi Kecenderungan Variabel Test and Trial Drive	80
20. Distribusi Frekuensi Variabel Customer Support Service	81
21. Distribusi Kecenderungan Variabel Customer Support Service	82
22. Hasil Uji Normalitas	82
23. Hasil Uji Linearitas	83
24. Hasil Uji Multikoleniaritas	83
25. Hasil Uji Heteroskedastisitas	84
26. Hasil Uji Regresi Berganda	85
27. Ringkasan Sumbangan Relatif dan Sumbangan Efektif	89

DAFTAR GAMBAR

Gambar	Halaman
1. <i>Internet Banking Map</i>	5
2. <i>IT Security</i>	7
3. Paradigma Penelitian	48

DAFTAR GRAFIK

Grafik	Halaman
1. Pengguna <i>Internet</i> di Indonesia	3

DAFTAR LAMPIRAN

Lampiran	Halaman
1. Instrumen Penelitian	112
2. Uji Validitas dan Uji Reliabilitas	137
3. Uji Prasyarat Analisis	139
4. Hasil Analisis Data	145
5. Perhitungan Distribusi Frekuensi	147
6. Perhitungan Sumbangan Relatif dan Sumbangan Efektif	153

BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi pada globalisasi ini semakin berkembang sebagai fasilitas pendukung yang digunakan pada aktivitas manusia. Pada kehidupan kini, teknologi tidak dapat dipisahkan dari kehidupan masyarakat, seakan-akan merupakan kebutuhan mendasar. Di zaman sekarang dimana kehidupan terlalu dipengaruhi oleh teknologi terutama internet. Semakin berkembangnya zaman terutama melalui internet, banyak inovasi-inovasi yang muncul di berbagai bidang kehidupan manusia, khususnya dalam dunia bisnis. Manusia sekarang menganggap bahwa dengan internet pekerjaan dan kebutuhan mereka dapat terpenuhi secara efektif dan efisien.

Internet (*Interconnection Networking*) merupakan seluruh jaringan yang saling terhubung secara fisik dan memiliki kemampuan untuk membaca dan menguraikan protokol komunikasi sehingga memungkinkan terjalannya komunikasi dan interaksi antara satu dengan yang lain di seluruh dunia tanpa dibatasi oleh ruang, waktu, tenaga, dan biaya. Indonesia sendiri menduduki peringkat ke-5 dari 20 negara dengan jumlah pengguna internet tertinggi. Dan pengguna internet di Indonesia tiap tahunnya juga selalu mengalami peningkatan.

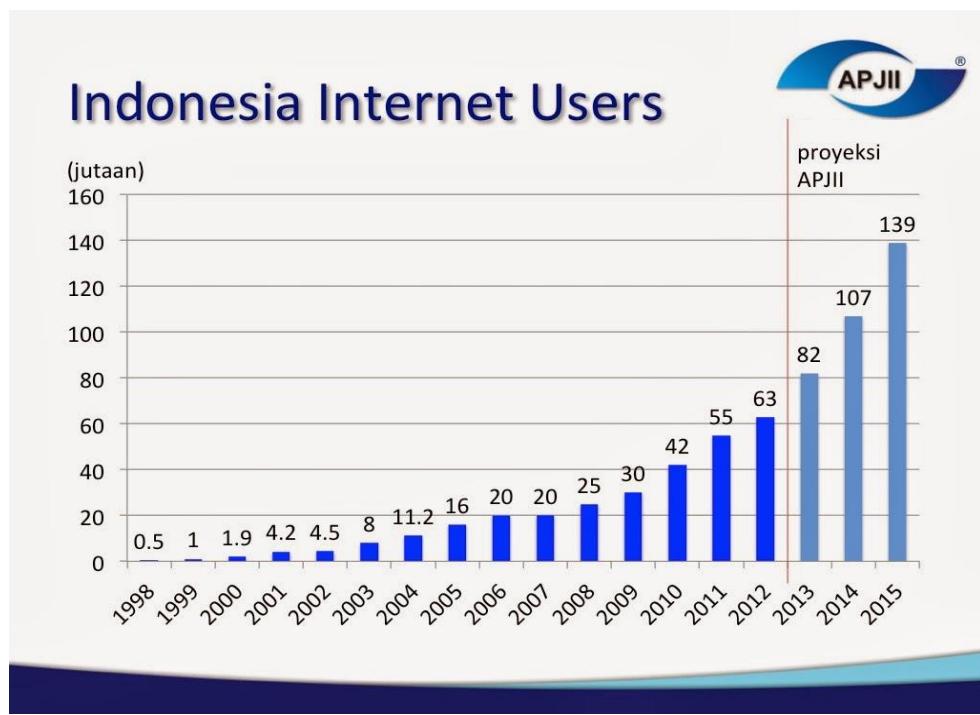
Tabel 1. Top 20 Negara dengan Jumlah Pengguna *Internet* Tertinggi per 30 Juni 2016

TOP 20 COUNTRIES WITH HIGHEST NUMBER OF INTERNET USERS - JUNE 30, 2016						
#	Country or Region	Population, 2016 Est.	Internet Users 30 June 2016	Internet Penetration	Growth (%) 2000 - 2016	Facebook 30 June 2016
1	China	1,378,561,591	721,434,547	52.3 %	3,106.4 %	1,800,000
2	India	1,266,883,598	462,124,989	36.5 %	9,142.5 %	157,000,000
3	United States	323,995,528	286,942,362	88.6 %	200.9 %	201,000,000
4	Brazil	206,050,242	139,111,185	67.5 %	2,682.2 %	111,000,000
5	Indonesia	258,316,051	132,700,000	51.4 %	6,535.0 %	88,000,000
6	Japan	126,464,583	115,111,595	91.0 %	144.5 %	26,000,000
7	Russia	146,358,055	103,147,691	70.5 %	3,227.3 %	12,000,000
8	Nigeria	186,879,760	97,210,000	52.0 %	48,505.0 %	16,000,000
9	Germany	80,722,792	71,727,551	88.9 %	198.9 %	31,000,000
10	Mexico	123,166,749	69,000,000	56.0 %	2,443.9 %	69,000,000
11	Bangladesh	162,855,651	63,290,000	38.9 %	63,190.0 %	21,000,000
12	United Kingdom	64,430,428	60,273,385	93.5 %	291.4 %	39,000,000
13	Iran	82,801,633	56,700,000	68.5 %	22,580.0 %	17,200,000
14	France	66,836,154	55,860,330	83.6 %	557.2 %	33,000,000
15	Philippines	102,624,209	54,000,000	52.6 %	2,600.0 %	54,000,000
16	Vietnam	95,261,021	49,063,762	51.5 %	24,431.9 %	40,000,000

Sumber: <https://proxisgroup.com/articles/waspadailah-hantaman-serangan-cyber-terhadap-indonesia/>

Perkembangan dan pemanfaatan teknologi Internet di Indonesia semakin hari semakin pesat. Dalam tabel di atas disajikan bahwa dari 20 negara dengan pengguna internet tertinggi, Indonesia menduduki peringkat kelima dengan jumlah penggunanya per 30 Juni 2016 yaitu sebesar 132.700.000 pengguna. Peningkatan kegiatan *e-banking* (*internet banking*, *mobile banking*, *sms banking*), *e-ducation*, *e-commerce*, *e-government*, *e-library* dan hal-hal lainnya sehari-hari yang dapat membantu aktivitas lebih cepat, efektif, dan efisien dimanapun dan kapanpun.

Setiap tahun pengguna Internet di Indonesia selalu mengalami peningkatan, mengingat semakin banyaknya inovasi yang dibuat dengan berbasis internet. Banyak pihak yang dengan sengaja melakukan inovasi yang memanfaatkan kemajuan teknologi ini. Bisa dilihat pada grafik di bawah, terlihat bahwa semakin tahun peningkatan pengguna internet di Indonesia naik secara signifikan dari tahun 1998 sampai dengan tahun 2015.



Sumber: Asosiasi Penyedia Jasa Internet Indonesia

Grafik 1. Pengguna *Internet* di Indonesia dari tahun 1998-2015.

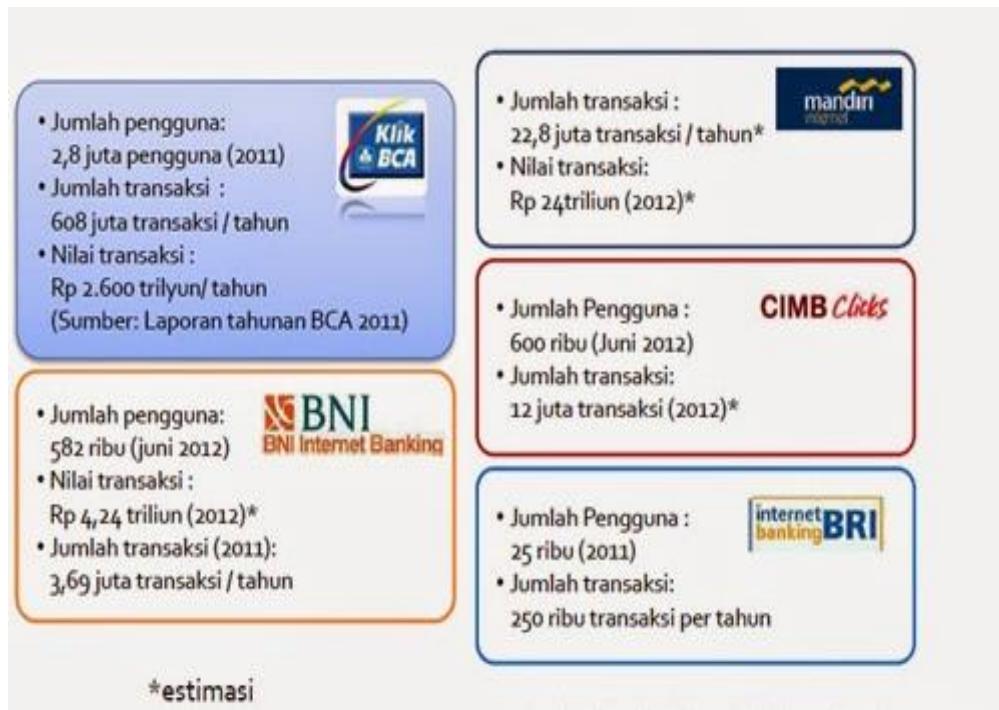
Penggunaan teknologi yang semakin maju saat ini membuat berbagai pihak berlomba-lomba menciptakan suatu inovasi yang sangat diminati masyarakat. Salah satu inovasi yang diciptakan tersebut yaitu dalam bidang perbankan. Dahulu, apabila kita ingin mengambil uang, mentransfer uang, dan transaksi lainnya kita harus jauh-jauh pergi ke bank dan belum lagi harus mengantri bahkan dari pagi hingga siang. Seiring perkembangan zaman yang semakin maju, terciptalah inovasi dalam bidang perbankan ini berupa *e-banking* atau *electronic banking* yang berbasis internet.

Beberapa produk yang diciptakan dalam basis internet banking yaitu *Electronic Data Capture* atau EDC untuk transaksi jual beli melalui kartu kredit dan kartu debit, *mobile banking*, *phone banking*, ada juga *video banking* yang bisa digunakan untuk bertatap muka langsung dengan teller bank. *Internet*

banking ini dapat digunakan untuk bermacam-macam aktivitas seperti pengecekan saldo rekening, pembayaran tagihan-tagihan seperti listrik dan telepon, transfer dana antar rekening atau antar bank, hingga pemesanan tiket.

Semakin beragamnya fasilitas yang disediakan melalui *internet banking*, maka semakin mendorong nasabah untuk menggunakan *internet banking*. Semakin majunya teknologi ini, sektor perbankan harus meningkatkan kinerja dan fasilitas-fasilitas lain dalam penggunaan *internet banking* di Indonesia. Produk dan jasa yang disediakan oleh pihak bank tersebut harus sesuai ketentuan yang ada berdasarkan jenis banknya sebagaimana yang diatur dalam Undang-undang Nomor 7 Tahun 1992 tentang perbankan sebagaimana telah diubah dengan Undang-undang Nomor 10 tahun 1998.

Saat ini pun semakin banyak pihak bank yang sudah menyediakan fasilitas *internet banking* bagi nasabah-nasabahnya seperti yang ditunjukkan gambar di bawah. Tujuan dari adanya *internet banking* ini diharapkan supaya kegiatan-kegiatan nasabah yang ada kaitannya dengan urusan transaksi-transaksi dan perbankan bisa dilakukan lebih mudah, dimana saja dan kapan saja.



Sumber:<https://sharingvision.com/keamanan-dan-kemudahan-survei-jumlah-pengguna-internet-banking-2011-2012/>

Gambar 1. Bank Penyedia Fasilitas *Internet Banking* dengan Estimasi Penggunanya tahun 2011-2012.

Kehadiran layanan *internet banking* telah menawarkan sejumlah fleksibilitas dan kemudahan dalam melakukan transaksi, baik antara bank dan nasabahnya, bank dengan *merchant*, bank dengan bank dan nasabah dengan nasabahnya. Fasilitas *internet banking* ini tentunya semakin memudahkan para nasabahnya untuk melakukan transaksi perbankan tanpa harus datang ke bank secara langsung. *Internet banking* juga memberikan akomodasi kegiatan perbankan melalui jaringan komputer kapan saja dan dimana saja dengan cepat, mudah, dan aman karena didukung oleh sistem pengamanan yang kuat. Hal ini berguna untuk menjamin keamanan dan kerahasiaan data serta transaksi yang dilakukan oleh nasabah. Selain itu, dengan *internet banking*, bank bisa meningkatkan kecepatan layanan dan jangkauan dalam aktivitas perbankan.

Dalam perkembangan teknologi perbankan seperti *internet banking*, pihak bank harus memperhatikan aspek perlindungan nasabah khususnya keamanan yang berhubungan dengan privasi nasabah. Keamanan layanan *online* ada empat, yaitu keamanan koneksi nasabah, keamanan data transaksi, keamanan koneksi *server*, dan keamanan jaringan sistem informasi dari *server*. Aspek penyampaian informasi produk perbankan sebaiknya disampaikan secara proporsional, artinya bank tidak hanya menginformasikan keunggulan atau kekhasan produknya saja, tapi juga sistem keamanan penggunaan produk yang ditawarkan.

Di balik kemudahan yang didapat dari penggunaan *internet banking*, ada juga resiko yang didapat dalam penggunaan layanan ini, antara lain banyak terjadi pelanggaran hukum menyangkut data pribadi melalui *internet* dan juga mengenai resiko finansial yang diderita oleh nasabah bank dalam penggunaan *internet banking* karena ulah para pelaku kejahatan TI, kejahatan seperti ini sering juga disebut sebagai *cybercrime*, bahkan lebih jauh lagi adalah dimanfaatkannya kecanggihan teknologi informasi dan komputer oleh pelaku kejahatan untuk tujuan pencucian uang dan kejahatan terorisme. Oleh karenanya banyak terjadi tindak kejahatan khususnya dengan produk internet banking ini, pihak industri perbankan harus mampu menyiapkan *security features* yang mampu menjaga tingkat kepercayaan masyarakat bahwa transaksi elektronik aman. Indonesia sendiri dianggap sebagai negara paling beresiko mengalami serangan IT *security* berdasarkan sumber dari *Security Threat Report* di tahun 2013.



Sumber:<https://itgid.org/serangan-cyber-crime-di-indonesia/>

Gambar 2. Indonesia Dianggap Negara yang Beresiko Mengalami Serangan IT Security pada tahun 2013.

Dalam prakteknya saat ini perlindungan atas privasi data/informasi pribadi dalam transaksi *online* di internet dapat diperoleh berdasarkan peraturan perundang-undangan yang ada, misalnya Undang-undang Perlindungan Data atau Undang-undang lainnya yang mengatur pula mengenai perlindungan privasi data pribadi. Selain itu, perlindungan hukum juga dapat diperoleh berdasarkan peraturan yang dibuat oleh situs misalnya kebijakan privasi (*privacy policy*), *privacy notice*, *privacy statement* maupun ketentuan pelayanan situs. Salah satu tujuan penting dari adanya undang-undang mengenai perlindungan privasi data adalah untuk menjamin bahwa setiap individu mempunyai kemampuan untuk mengawasi dan mengakses informasi pribadi mereka yang dikumpulkan oleh pihak lain serta untuk memberikan perbaikan jika diperlukan.

Bentuk-bentuk kejahatan yang sering terjadi dalam sektor perbankan yaitu *man in the middle attack* dan *trojan horses* yang dapat menganggu keamanan layanan. Gambaran umum dari aktivitas yang sering disebut *man in the middle attack* yaitu penyerang membuat sebuah *website* dan membuat nasabah pengguna layanan *internet banking* atau *user* masuk ke *website* tersebut. Agar berhasil mengelabui *user*, *website* tersebut harus dibuat semirip mungkin dengan *website* bank yang sebenarnya. Untuk mengecoh *token*, penyerang dapat mengirimkan *challenge-response* kepada *user* sebelum melakukan transaksi illegal. Sedangkan, *trojan horses* adalah program palsu dengan tujuan jahat yang disusupkan kepada sebuah program yang umum dipakai. Di sini para penyerang meng-*install trojan* ke komputer *user*. Ketika *user* mulai *login* ke *website* banknya, penyerang menumpangi sesi tersebut melalui *trojan* untuk melakukan transaksi yang diinginkannya. *Trojan Horse* berbeda dengan virus yang merusak lainnya, *trojan horses* tidak dapat diketahui keberadaannya.

Perlunya sosialisasi aktif dari perbankan kepada masyarakat atau nasabah dan pegawai perbankan mengenai bentuk-bentuk kejahatan yang dapat terjadi dengan produk atau layanan yang disediakannya. Saat ini sudah terdapat teknologi dan peraturan hukum yang dapat membuat *internet banking* menjadi aman, akan tetapi pihak perbankan dan pemerintah perlu terus mengupayakan agar penyelenggaraan *internet banking* lebih aman dan terjamin. Namun, saat ini terdapat kesan bahwa para pelaku usaha perbankan dan masyarakat pada umumnya kurang *aware* dan peduli terhadap proses penanganan kasus-kasus

tindak pidana *internet banking*. Maka dari itu perlu dilakukan upaya-upaya menyeluruh dari semua pihak untuk menuju ke arah yang lebih baik.

Peneliti memilih lokasi untuk penelitian yaitu di D.I. Yogyakarta dengan mempertimbangkan hal bahwa pengguna internet di wilayah D.I. Yogyakarta cukup tinggi. Direktur Utama (dirut) PT Telkom, Arwin Rasyid (Detik, 19 Oktober 2005) mengatakan:

“Pengguna internet di wilayah Yogyakarta mencapai 17 persen. Cukup tinggi dibanding dengan penggunaan rata-rata nasional yang hanya 5 persen. Tingginya angka pengguna internet itu karena Yogyakarta sebagai kota pendidikan sehingga orang yang melek internet pun lebih banyak”.

Berdasarkan uraian di atas, penulis tertarik untuk mengadakan penelitian dengan judul: **“Pengaruh Penggunaan *Internet Banking* dan Perlindungan Nasabah Pengguna Fasilitas *Internet Banking* terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta (DIY).”**

B. Identifikasi Masalah

Berdasarkan latar belakang masalah dapat diidentifikasi permasalahan yang ada pada penggunaan *internet banking* dan perlindungan nasabah terhadap *cyber crime* sebagai berikut:

1. Kemajuan teknologi informasi yang menuntut banyaknya inovasi terbaru di berbagai bidang khususnya bidang perbankan membuat banyak pihak bank bersaing untuk memberikan layanan terbaiknya.
2. Produk dan layanan *internet banking* yang semakin memudahkan nasabah dalam melakukan transaksi juga menimbulkan banyak resiko kejahatan *cyber* seperti *carding*, *hacking*, atau *pun cracking*.

3. Bentuk-bentuk kejahatan *cyber crime* dalam bidang perbankan.
4. Keamanan layanan *online* yang disediakan pihak bank untuk mencegah terjadinya kejahatan *cyber* yang belum secara maksimal dilaksanakan oleh pihak bank. Hal ini ditunjukkan dengan masih banyaknya kejahatan online yang terjadi di dunia perbankan.
5. Bentuk perlindungan yang seharusnya dilakukan pihak bank untuk melindungi data transaksi nasabah dari kejahatan IT harus lebih diperketat agar data nasabah pengguna *internet banking* tidak mudah di *hack* oleh para *hacker* maupun pelaku kejahatan *cyber* lainnya.

C. Batasan Masalah

Agar penilitian ini lebih fokus maka permasalahan penelitian dibatasi pada permasalahan yang berkaitan dengan penggunaan *internet banking* dan perlindungan nasabah bank pengguna fasilitas *internet banking* terhadap *cyber crime* di wilayah DIY.

D. Rumusan Masalah

1. Bagaimana pengaruh penggunaan *internet banking* terhadap *cyber crime* di wilayah D.I. Yogyakarta?
2. Bagaimana pengaruh perlindungan nasabah bank dalam penggunaan fasilitas *internet banking* terhadap *cyber crime* di wilayah D.I. Yogyakarta?
3. Bagaimana pengaruh penggunaan *internet banking* dan perlindungan nasabah bank dalam penggunaan fasilitas *internet banking* terhadap *cyber crime* di wilayah D.I. Yogyakarta?

E. Tujuan Penelitian

Berdasarkan perumusan masalah diatas, tujuan yang hendak dicapai penulis adalah sebagai berikut:

1. Untuk mengetahui pengaruh penggunaan *internet banking* terhadap *cyber crime* di wilayah D.I. Yogyakarta.
2. Untuk mengetahui pengaruh perlindungan nasabah bank dalam penggunaan fasilitas *internet banking* terhadap *cyber crime* di wilayah D.I. Yogyakarta.
3. Untuk mengetahui pengaruh penggunaan *internet banking* dan perlindungan nasabah bank dalam penggunaan fasilitas *internet banking* terhadap *cyber crime* di wilayah D.I. Yogyakarta.

F. Manfaat Penelitian

Penulis berharap bahwa kegiatan penelitian dalam penulisan ini akan bermanfaat bagi penulis maupun pihak lain. Adapun manfaat yang dapat diperoleh dari penulisan ini antara lain:

1. Manfaat Teoritis
 - a. Hasil penelitian ini diharapkan dapat bermanfaat dalam pengembangan ilmu pengetahuan di bidang ilmu ekonomi pada umumnya dan perbankan pada khususnya, serta dapat dipakai sebagai acuan terhadap penulisan maupun penelitian sejenis untuk tahap berikutnya.
 - b. Hasil penelitian ini diharapkan dapat memperkaya referensi dan literatur dalam dunia kepustakaan tentang Perlindungan Nasabah Bank dalam Penggunaan Fasilitas *Internet Banking* terhadap *Cyber Crime* di D.I. Yogyakarta.

2. Manfaat Praktis

- a. Memberikan bahan masukan bagi pihak bank maupun pemerintah mengenai perlindungan hukum bagi nasabah akan terjadinya tindak kejahatan *cyber crime* dalam *internet banking*.
- b. Memberikan pendalaman, pengetahuan, dan pengalaman baru kepada penulis mengenai permasalahan yang dikaji tersebut, sehingga dapat berguna bagi penulis maupun orang lain di kemudian hari.
- c. Sebagai bahan masukan agar adanya payung hukum yang bisa ditegakkan yang lebih khusus menangani kejahatan *cyber* mengingat kini sudah memasuki era digital.

BAB II

KAJIAN PUSTAKA

A. Kajian Teori

1. Tinjauan Umum tentang *Cyber Crime*

a. Pengertian *Cyber Crime*

Apabila kita berbicara mengenai kejahatan berteknologi tinggi seperti kejahatan internet atau *cybercrime*, seolah-olah hukum itu ketinggalan dari peristiwanya. Seiring dengan berkembangnya pemanfaatan internet, maka mereka yang memiliki kemampuan dibidang komputer dan memiliki maksud-maksud tertentu dapat memanfaatkan komputer dan internet untuk melakukan kejahatan atau kenakalan yang merugikan pihak lain.

Dalam dua dokumen konferensi PBB mengenai *The Prevention of Crime and The Treatment of Offenders* di Havana, Cuba pada tahun 1990, dan di Wina, Austria pada tahun 2000, ada dua istilah yang dikenal yaitu: “*cybercrime*” dan “*computer related crime*”. Dalam *background paper* untuk lokakarya konferensi PBB X/2000 di Wina, Austria, istilah *cybercrime* dibagi dalam dua kategori, yaitu pertama, *cybercrime* dalam arti sempit disebut *computer crime*, kedua *cybercrime* dalam arti luas disebut *computer related crime*. *Cybercrime* meliputi kejahatan, yaitu yang dilakukan:

- 1) Dengan menggunakan sarana-sarana dari sistem atau jaringan komputer (*by means of computer system or network*)

- 2) Di dalam sistem atau jaringan komputer (*in a computer system or network*) dan
- 3) Terhadap sistem atau jaringan komputer (*against a computer system or network*).

Dari definisi tersebut, maka dalam arti sempit *cybercrime* adalah *computer crime* yang ditujukan terhadap sistem atau jaringan, sedangkan dalam arti luas *cybercrime* mencakup seluruh bentuk kejahatan yang ditujukan kepada komputer, jaringan komputer dan penggunanya serta bentuk-bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer.

Secara garis besar kejahatan-kejahatan yang terjadi terhadap suatu sistem atau jaringan komputer dan yang menggunakan komputer juga dapat terjadi didunia perbankan. Kegiatan yang potensial yang menjadi target *cybercrime* dalam kegiatan perbankan antara lain adalah:

- 1) Layanan pembayaran menggunakan kartu kredit pada situs-situs toko online.
- 2) Layanan perbankan online (*on-line banking*).

Dalam kaitannya dengan *cybercrime*, maka sudut pandangnya adalah kejahatan internet yang menjadikan pihak bank, merchant, toko online atau nasabah sebagai korban, yang dapat terjadi karena maksud jahat seseorang yang memiliki kemampuan dalam bidang teknologi informasi, atau seseorang yang memanfaatkan kelengahan pihak bank, pihak merchant maupun pihak nasabah.

b. Bentuk Potensi *Cyber Crime* dalam Kegiatan Perbankan

Beberapa bentuk potensi *cyber crime* dalam kegiatan perbankan antara lain:

- 1) *Typo site*, pelaku membuat nama situs palsu yang sama persis dengan situs asli dan membuat alamat yang mirip dengan alamat situs asli. Pelaku menunggu kesempatan jika seseorang korban salah mengetikkan alamat dan masuk kesitus palsu buatannya. Jika hal ini terjadi maka pelaku akan memperoleh informasi *user* dan *password* korbannya, dan dapat dimanfaatkan untuk merugikan korban.
- 2) *Keylogger/keystroke logger*: Modus lainnya adalah *keylogger*. Hal ini sering terjadi pada tempat mengakses internet umum seperti di warnet. Program ini akan merekam karakter-karakter yang diketikkan oleh *user* dan berharap akan mendapatkan data penting seperti *user ID* maupun *password*. Semakin sering mengakses internet di tempat umum, semakin rentan pula terkena modus operandi yang dikenal dengan istilah *keylogger* atau *keystroke recorder* ini. Sebab komputer-komputer yang ada di warnet digunakan berganti-ganti oleh banyak orang. Cara kerja dari modus ini sebenarnya sangat sederhana, tetapi banyak para pengguna komputer ditempat umum yang lengah dan tidak sadar bahwa semua aktifitasnya dicatat oleh orang lain. Pelaku memasang program *keylogger* dikomputer-komputer umum, program *keylogger* ini akan merekam semua tombol keyboard yang ditekan oleh pengguna komputer berikutnya. Di lain waktu, pemasang

keylogger akan mengambil hasil “jebakannya” dikomputer yang sama, dan dia berharap akan memperoleh informasi penting dari para korbannya, semisal *user ID* dan *password*.

- 3) *Sniffing*: usaha untuk mendapatkan *user ID* dan *password* dengan jalan mengamati paket data yang lewat pada jaringan komputer.
- 4) *Brute Force Attacking*: Usaha untuk mendapatkan password atau key dengan mencoba semua kombinasi yang mungkin.
- 5) *Web Deface*: *System Exploitation* dengan tujuan mengganti tampilan halaman muka satu situs.
- 6) *Email Spamming*: Mengirimkan junk email berupa iklan produk dan sejenisnya pada alamat email seseorang.
- 7) *Daniel of Service*: Membanjiri data dalam jumlah sangat besar dengan maksud untuk melumpuhkan sistem sasaran.
- 8) *Virus worm, trojan*: Menyebarluaskan *virus worm* maupun *trojan* dengan tujuan untuk melumpuhkan sistem komputer, memperoleh data-data dari sistem korban dan untuk mencemarkan nama baik pembuat perangkat lunak tertentu.

Contoh *cybercrime* dalam transaksi perbankan yang menggunakan sarana internet sebagai basis transaksi adalah sistem layanan kartu kredit dan layanan perbankan *online (on-line banking)*. Dalam sistem layanan yang pertama, yang perlu diwaspadai adalah tindak kejahatan yang dikenal dengan istilah *carding*. Prosesnya adalah sebagai berikut, pelaku *carding* memperoleh data kartu kredit korban secara tidak sah

(*illegal interception*), dan kemudian menggunakan kartu kredit tersebut untuk berbelanja di toko online (*forgery*). Modus ini dapat terjadi akibat lemahnya sistem autentifikasi yang digunakan dalam memastikan identitas pemesanan barang di toko *online*.

Kegiatan yang kedua adalah perbankan on-line (*on-line banking*). Modus yang pernah muncul di Indonesia dikenal dengan istilah *typosite* yang memanfaatkan kelengahan nasabah yang salah mengetikkan alamat bank *on-line* yang ingin diaksesnya. Pelakunya sudah menyiapkan situs palsu yang mirip dengan situs asli bank *on-line* (*forgery*). Jika ada nasabah yang salah ketik dan masuk ke situs palsu tersebut, maka pelaku akan merekam *user ID* dan *password* nasabah tersebut untuk digunakan untuk mengaksesnya di situs yang sebenarnya (*illegal acces*) dengan maksud untuk merugikan nasabah.

c. Jenis-jenis *Cyber Crime*

Berdasarkan jenis aktifitas yang dilakukannya, *cybercrime* dapat digolongkan menjadi beberapa jenis:

1) *Hacking*

Kegiatan menerobos program komputer milik orang/pihak lain. *Hacker* adalah orang yang gemar eksplorasi/ngorek komputer, memiliki keahlian membuat dan membaca program tertentu, dan terobsesi mengamati keamanannya. “*Hacker*” memiliki 2 wajah ganda: “*Hacker Budiman/White Hat Hacker*” memberi tahu kepada admin yang komputernya diterobos, bahwa adanya kelemahan-

kelemahan pada program yang dimiliki dan punya potensi disusup.

Karakteristik *White Hat Hacker* ini adalah memberikan informasi bukan merusak yang pasti menguntungkan/membantu korbannya.

“*Hacker Pencoleng/Black Hat Hacker*”, menerobos program orang lain untuk merusak, manipulasi/merubah serta mencuri datanya.

Karakteristik *Black Hat Hacker* ini adalah melakukan aktifitas kriminal yang pasti merugikan korbannya.

2) *Cracking*

Hacking untuk tujuan jahat. Sebutan pelaku *cracking* adalah “*cracker*”. Aktifitas *cracker* sejenis dengan “hacker bertopi hitam” (*Black Hat Cracker*). Berbeda dengan “*carder*” yang hanya mengintip kartu kredit, “*cracker*” mengintip simpanan para nasabah di berbagai bank atau pusat data sensitif lainnya untuk keuntungan diri sendiri. Meski sama-sama menerobos keamanan komputer orang lain, “*hacker*” lebih fokus pada prosesnya. Sedangkan “*cracker*” lebih fokus untuk menikmati hasilnya. Contoh kasus ini misalnya FBI bekerja sama dengan polisi Belanda dan polisi Australia menangkap seorang *cracker* remaja menerobos 50 ribu komputer dan mengintip 1,3 juta rekening berbagai bank di dunia.

3) *Carding*

Aktifitas berbelanja secara online tetapi menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara ilegal, pelaku *carding* biasa disebut *carder*. Biasanya para *carder* mencuri data

nasabah dengan menginjeksi komunikasi data pada *outlet* atau *store* yang sering melakukan transaksi *trading* menggunakan kartu kredit. Menurut riset Clear Commerce Inc, perusahaan teknologi informasi yang berbasis di Texas–Amerika Serikat, Indonesia memiliki “*carder*” terbanyak kedua di dunia setelah Ukraina. Sebanyak 20 persen transaksi melalui internet yang berasal dari Indonesia adalah hasil *carding*. Akibatnya, banyak situs belanja online yang memblokir IP address (alamat komputer *internet*) yang berasal dari Indonesia.

4) *Defacing*

Kegiatan mengubah halaman situs/*website* pihak lain, seperti yang terjadi pada situs Presiden SBY, Kemenkominfo dan Partai Golkar, BI dan situs KPU saat pemilu 2004 lalu. Banyaknya kasus *deface* saat ini yang bermotif iseng belaka mereka ingin unjuk kebolehan, pamer kemampuan membuat program, tapi ada juga pelaku *deface* yang jahat, mereka melakukan aktifitas *deface* untuk mencuri data dan dijual kepada pihak lain.

5) *Fishing* atau *Phising*

Kegiatan memancing pengguna *internet* dengan harapan agar user secara tidak sadar memberikan informasi data *user* dan *password* nya pada *website* yang sudah di-*deface*. *Phising* biasanya diarahkan kepada pengguna online *internet banking*. Targetnya adalah nasabah yang ingin bertransaksi *internet banking* kurang teliti dalam menulis *website*. Cara kerjanya peretas biasanya membeli banyak *domain*

plesetan dari bank yang menjadi target, sasarannya *user* merasa tidak menyadari telah salah mengetik alamat *website* namun tetap halaman awal *website* target dibuat sama seperti aslinya, akibat yang diharapkan oleh peretas nasabah mengisi *User ID* dan *password*. Setelah mengakses nasabah akan diberikan informasi gangguan terhadap server bank target, padahal itu bagian dari rekayasa peretas untuk membuat nasabah tidak menyadari kalau user dan passwordnya sudah diretas diambil oleh penyusup.

d. Hambatan dalam Penanganan *Cyber Crime*

Meskipun sudah ada beberapa pasal yang bisa menjerat pelaku *cybercrime* ke penjara, tetapi masih dijumpai adanya hambatan-hambatan dalam pelaksanaan di lapangan yang antara lain sebagai berikut:

1) Perangkat hukum yang belum memadai

Para penyidik (khususnya Polri) melakukan analogi atau perumpamaan dan persamaan terhadap pasal-pasal yang ada dalam KUHP sependapat bahwa perlu dibuat undang-undang yang khusus mengatur *cybercrime*.

2) Kemampuan penyidik

Secara umum penyidik Polri masih sangat minim dalam penguasaan operasional komputer dan pemahaman terhadap hacking komputer terhadap kasus-kasus itu. Beberapa faktor yang sangat berpengaruh (*determinan*) adalah:

a) Kurangnya pengetahuan tentang komputer.

b) Pengetahuan teknis dan pengalaman para penyidik dalam menangani kasus-kasus *cybercrime* masih terbatas.

c) Faktor sistem pembuktian yang menyulitkan para penyidik.

3) Alat Bukti

Persoalan alat bukti yang dihadapi di dalam penyidikan terhadap *cybercrime* antara lain berkaitan dengan karakteristik kejahatan *cybercrime* itu sendiri, yaitu; sasaran atau media *cybercrime* adalah data dan atau sistem komputer atau sistem internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelakunya. *Cybercrime* seringkali dilakukan hampir-hampir tanpa saksi, di sisi lain, saksi korban seringkali berada jauh di luar negeri sehingga menyulitkan penyidik melakukan pemeriksaan saksi dan pemberkasan hasil penyidikan.

4) Fasilitas komputer forensik

Untuk membuktikan jejak-jejak para *hacker*, dan *cracker* dalam melakukan aksinya terutama yang berhubungan dengan program-program dan data komputer, sarana Polri belum memadai karena belum ada komputer forensik. Fasilitas ini diperlukan untuk mengungkapkan data digital serta merekam dan menyimpan bukti-bukti berupa *soft copy* (*image*, program, dsb). Dalam hal ini Polri masih belum mempunyai fasilitas *forensic computing* yang memadai. Fasilitas *forensic computing* yang akan didirikan Polri diharapkan

akan dapat melayani tiga hal penting yaitu *evidence collection*, *forensic analysis*, *expert witness*.

2. Tinjauan Umum tentang Perbankan

a. Pengertian Bank dan Perbankan

Pengertian bank sering disamakan dengan pengertian perbankan.

Padahal dua hal yang sebenarnya berbeda. Bank hanya mencakup aspek kelembagaan. Ada beberapa pengertian ataupun definisi bank yaitu:

- 1) Menurut Joseph Sinkey bahwa yang dimaksud bank adalah *departement store of finance* yang menyediakan berbagai jasa keuangan.
- 2) Menurut *Dictionary of Banking and Financial Service* by Jerry Rosenberg bahwa yang dimaksud bank adalah lembaga yang menerima simpanan giro, deposito, dan membayar atas data dokumen yang ditarik pada orang atau lembaga tertentu, mendiskonto surat berharga, memberikan pinjaman dan menanamkan dananya dalam surat berharga.
- 3) Menurut UU No.10 Tahun 1998 (revisi UU No.14 Tahun 1992) bahwa yang dimaksud bank adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalirkannya kepada masyarakat dalam rangka meningkatkan taraf hidup rakyat banyak.

Bank adalah sebuah lembaga atau perusahaan yang aktivitasnya menghimpun dana berupa giro, deposito tabungan dan simpanan yang

lain dari pihak yang kelebihan dana kemudian menempatkannya kembali kepada masyarakat yang membutuhkan dana melalui penjualan jasa keuangan yang dapat meningkatkan kesejahteraan rakyat banyak.

Perbankan adalah segala sesuatu yang berkaitan dengan bank, mencakup kelembagaan, kegiatan usaha, serta cara dan proses dalam melaksanakan kegiatan usahanya. Kegiatan usaha tersebut adalah menyangkut jasa keuangan. Dalam perspektif ilmu keuangan, perbankan adalah bagian dari ilmu keuangan. Dengan demikian pembahasan manajemen perbankan memfokuskan pada masalah keuangan bukan bidang *marketing* maupun sumber daya manusia (Taswan, 2010: 6).

b. Pengertian Nasabah

Dalam Peraturan Bank Indonesia No. 7/7/PBI/2005 dan No. 10/10/PBI/2008 tentang penyelesaian pengaduan nasabah Pasal 1 angka 2 yang dimaksud dengan nasabah adalah pihak yang menggunakan jasa bank, termasuk pihak yang tidak memiliki rekening namun memanfaatkan jasa bank untuk melakukan transaksi keuangan (*walk-in costumer*). Di dalam UU No. 10 Tahun 1998 tentang Perbankan dimuat tentang jenis dan pengertian nasabah. Dalam Pasal 1 angka 17 disebutkan bahwa pengertian nasabah yaitu pihak yang menggunakan jasa bank. Jenis-jenis nasabah ada 2, yakni:

- 1) Nasabah Penyimpan, yakni nasabah yang menempatkan dananya di bank dalam bentuk simpanan berdasarkan perjanjian bank dengan nasabah yang bersangkutan.

2) Nasabah Debitur, yakni nasabah yang memperoleh fasilitas kredit atau pembiayaan berdasarkan prinsip syariah atau yang dipersamakan dengan itu berdasarkan perjanjian bank dengan nasabah yang bersangkutan.

c. Pengawasan Perbankan

Kebijakan pengawasan yang dilakukan oleh Bank Indonesia terhadap perbankan bertujuan untuk melindungi kepentingan masyarakat pemilik dan serta menjaga kelangsungan usaha bank sebagai kepercayaan dan sebagai lembaga intermediasi. Pengawasan tersebut dilaksanakan baik secara tidak langsung (*off-site supervisor*) maupun secara langsung (*on-site examination*). Pengawasan tidak langsung adalah pengawasan yang dilakukan dengan meneliti, menganalisis serta mengevaluasi laporan-laporan yang disampaikan oleh suatu bank dengan tujuan untuk mengetahui apakah bank telah melaksanakan ketentuan perbankan sekaligus untuk menilai kinerja perbankan. Sementara itu, yang dimaksud dengan pengawasan langsung adalah pengawasan dalam bentuk pemeriksaan langsung yang diikuti dengan tindakan-tindakan perbaikan. Sebagaimana diatur dalam undang-undang, seluruh bank wajib memberikan kesempatan kepada pemeriksa bank untuk memeriksa buku-buku serta berkas-berkas yang ada pada bank. Selain itu, bank juga wajib membantu apabila diperlukan dalam rangka memperoleh kebenaran dari segala keterangan, dokumen, dan penjelasan yang dilaporkan oleh bank yang bersangkutan.

2. Tinjauan Umum tentang *Internet Banking*

a. Pengertian *Internet Banking*

Internet merupakan sekumpulan jaringan yang terhubung satu dengan lainnya, di mana jaringan menyediakan sambungan menuju global informasi. Sedangkan *internet banking* merupakan suatu bentuk pemanfaatan media internet oleh bank untuk mempromosikan dan sekaligus melakukan transaksi secara *online*, baik dari produk yang sifatnya konvensional maupun yang baru. *Internet banking* sebagai bentuk pelayanan bank melalui media internet. Kehadiran *internet banking* telah menyebabkan efisiensi penyelenggaraan kegiatan usaha bank sangat tinggi. *Internet banking* memiliki tiga tahap pelayanan yang ditawarkan kepada nasabah, yaitu layanan informasi (*informational*) dimana bank hanya menyediakan informasi jasa keuangan dalam *websitenya*, komunikasi (*communicational*) dimana dalam *website* tersebut juga memungkinkan nasabah untuk dapat berkomunikasi dengan bank, transaksi (*transactional/advance*) dimana sudah memungkinkan nasabah untuk melakukan transaksi-transaksi keuangan virtual seperti, transfer dana, pengecekan saldo, ataupun jenis pembayaran.

b. Tujuan *Internet Banking*

Media internet dapat digunakan oleh bank untuk beberapa tujuan, baik bagi pihak bank maupun pihak nasabah, yaitu:

- 1) Bagi Bank

- a) Menjelaskan produk dan jasa seperti, pemberian pinjaman dan kartu kredit.
- b) Menyediakan informasi mengenai suku bunga dan kurs mata uang asing yang terbaru.
- c) Menunjukkan laporan tahunan perusahaan dan keterangan pers lainnya.
- d) Menyediakan informasi ekonomi dan bisnis seperti perkiraan bisnis.
- e) Memberikan daftar lokasi kantor bank tersebut dan lokasi ATM.
- f) Memberikan daftar pekerjaan yang membutuhkan tenaga kerja baru.
- g) Memberikan gambaran mengenai bank.
- h) Menyediakan informasi mengenai sejarah bank dan peristiwa terbaru.
- i) Memberikan pelayanan kepada nasabah untuk memeriksa neraca tabungan dan memindahkan dana antar tabungan.
- j) Menyediakan algoritma yang sederhana sehingga para nasabah dapat membuat perhitungan untuk pembayaran pinjaman, perubahan atau pengurangan pembayaran hipotik, dan lain sebagainya (Mary J.Cronin dalam Niko Estradiyanto, 2012).

2) Bagi Nasabah

- a) Mempermudah nasabah dalam bertransaksi perbankan, karena dengan *internet banking* akses perbankan dapat dilakukan di

komputer pribadi (*personal computer*) nasabah bahkan lebih dekat, tanpa harus datang ke kantor cabang.

- b) Mempercepat kegiatan transaksi perbankan hanya dengan modal komputer pribadi, nasabah dapat mengakses transaksi apapun dengan beberapa “klik” di *mouse* komputer. Tanpa membuang-buang waktu untuk datang mengisi formulir di kantor cabang.
- c) Menghemat biaya seperti menghemat ongkos jalan ke kantor cabang.

c. Faktor-faktor yang Mempengaruhi Penggunaan *Internet Banking*

Faktor-faktor yang mempengaruhi untuk menggunakan *internet banking* yaitu:

1) Kenyamanan (*Convenience*)

Kenyamanan berarti nasabah merasa bahwa *internet banking* itu fleksibel dalam hal waktu dan tempat. *Internet banking* menyediakan tingkat kenyamanan yang lebih tinggi yang memudahkan nasabah untuk melakukan transaksi perbankan kapanpun dan dimanapun.

2) Kemampuan Mengakses (*Accessability*)

Kemampuan mengakses adalah kemampuan untuk mengakses situs dan menghubungi pihak bank ketika dibutuhkan.

3) Ketersediaan Fitur (*Feature Availability*)

Faktor lain yang penting di dalam kesuksesan *e-banking*, yaitu kemampuan inovasi untuk menghadapi kebutuhan nasabah dengan menggunakan ketersediaan fitur yang berbeda pada *website*. Fitur

berarti hal-hal apa saja yang dapat dilakukan oleh nasabah dengan menggunakan *internet banking*.

4) Privasi (*Privacy*)

Kerahasiaan (*privacy*) berarti segala hal yang berkaitan dengan informasi pribadi pengguna terjamin kerahasiaannya, tidak ada orang yang mengetahuinya.

5) Kecepatan (*Speed*)

Kecepatan dapat diartikan dengan kecepatan internet banking untuk memberikan informasi yang diinginkan pengguna *internet banking*.

6) Tarif dan Biaya (*Fees and Charge*)

Internet banking memiliki biaya transaksi yang murah dan layanan kecepatan tinggi jika dibandingkan dengan layanan perbankan lain.

Internet banking memudahkan para nasabah untuk mengakses akun bank mereka, biaya *service* yang lebih rendah, dan penghematan waktu.

7) Manajemen dan Citra Bank (*Bank Management and Image*)

Reputasi atau lebih dikenal dengan *brand reputation* sering didefinisikan sebagai persepsi kualitas yang digabungkan dengan nama. Pada bisnis-bisnis industri dan jasa, nama (merk) lebih sering dihubungkan dengan reputasi perusahaan daripada dengan produk atau jasa itu sendiri. Karena itulah salah satu pertimbangan nasabah dalam menabung dan menggunakan jasa bank adalah reputasi perusahaan tersebut di mata nasabah, karena kepercayaan merupakan

salah satu faktor utama bagi nasabah untuk mempercayakan uangnya di tabung atau di investasikan pada bank tersebut.

8) Desain (*Design*)

Desain didefinisikan sebagai tampilan dari *internet banking* semakin tinggi tingkat komunikasi sosial yang ditampilkan oleh suatu *website* bank, semakin besar pengaruhnya pada kepercayaan konsumen dan meningkatkan kemungkinan konsumen melakukan transaksi online.

9) Konten (*Content*)

Konten merupakan kemampuan *internet banking* untuk menyediakan informasi yang terbaru mengenai produk maupun jasa terbaru yang ditawarkan.

d. Produk atau Jasa *Internet Banking*

Secara umum terdapat beberapa jenis produk/jasa yang ditawarkan melalui *internet banking*:

- 1) Informasi saldo
- 2) Pembukaan rekening
- 3) Transfer

Transfer dengan menggunakan jasa *internet banking* adalah cara yang paling efisien dan murah karena nasabah dapat melakukannya dimana saja dan tidak dibatasi oleh waktu.

4) *Payment Gateway*

Merupakan fasilitas pembayaran jasa *internet banking* (antara lain pembayaran telepon, air PAM, dan listrik) yang disediakan oleh bank

sehingga nasabah dapat melakukan pembayaran langsung melalui *internet*. Konsep *payment gateway* ini mirip dengan transfer karena nasabah maupun penyedia jasa (perusahaan telepon atau listrik) harus sama-sama memiliki *account* di bank tersebut. Dengan demikian selain nasabah bank tersebut, orang lain tetap saja tidak bisa melakukan transaksi *payment gateway*. Bahkan saat ini telah berkembang layanan *account aggregation* yaitu jasa bank yang menyatukan informasi dari berbagai *website* dan menampilkan informasi tersebut dalam format terkonsolidasi kepada nasabah. Informasi dapat berkisar dari informasi untuk konsumsi publik hingga informasi rekening pribadi nasabah. *Account aggregation* banyak digunakan untuk layanan *bill presentment and payment*, dimana nasabah mendeklarasikan kepada bank atau pihak ketiga untuk mendebet rekening milik nasabah untuk melakukan pembayaran sejumlah tagihan milik nasabah, misalnya tagihan listrik, telepon, dll. Untuk itu nasabah perlu menyerahkan *Personal Identification Number* serta *password* miliknya kepada bank atau pihak ketiga.

5) Kliring

6) *Trade Services and Finance*

7) Penutupan rekening

8) Transaksi lainnya

Bank penyedia *internet banking* dapat juga menyediakan pelayanan jasa bagi korporasi seperti *cash management service*, *continous link*

settlement, pemesanan buku cek bahkan nasabah dapat memperoleh informasi, berita, analisis seputar *foreign exchange transaction* serta juga dapat melakukan *transaksi spot, swap, forward*, dll melalui *internet banking*. Selain itu bank dapat memberikan pelayanan lainnya di luar produk perbankan seperti misalnya nasabah dapat membeli voucher isi ulang telepon genggam dengan langsung mendebet rekening nasabah yang bersangkutan, pembelian saham secara online, pembayaran polis asuransi dan sebagainya.

e. Sistem Keamanan *Internet Banking*

Kesempatan Indonesia untuk mengembangkan *internet banking* sangat terbuka luas. Hal itu dimungkinkan karena pertumbuhan penggunaan internet di kawasan Asia sangat tinggi dan nasabah perbankan juga memerlukan pelayanan yang lebih baik (Abdul Wahid, dalam Niko Astradiyanto, 2012).

Salah satu isu yang menjadi permasalahan dalam penggunaan *internet banking* adalah sistem keamanan bertransaksi perbankan dengan menggunakan internet. Masalah yang paling sering muncul adalah adanya pencurian nomor kartu kredit. Nomor curian ini kemudian dimanfaatkan oleh orang yang sesungguhnya tidak berhak. Nasabah harus diyakinkan oleh pihak bank bahwa transaksi perbankan bahwa transaksi perbankan berjalan aman karena bank bersangkutan memiliki perangkat keamanan untuk mencegah para *hacker* mengganggu transaksi

mereka. Ada dua jenis sistem keamanan yang dipakai dalam *internet banking* yaitu (Mary J.Cronin dalam Niko Estradiyanto, 2012).

1) Sistem *Cryptography*

Sistem ini menggunakan angka-angka yang dikenal dengan kunci (*key*). Sistem ini disebut dengan sistem sandi. Ada dua tipe *cryptography* yaitu simetris dan asimetris. Pada sistem simetris ini menggunakan kode kunci yang sama bagi penerima dan pengirim pesan. Kelemahan dari *cryptography* simetris adalah kunci ini harus dikirim kepada pihak penerima dan hal ini memungkinkan seseorang untuk mengganggu ditengah jalan. Sistem *cryptography* asimetris juga mempunyai kelemahan yaitu jumlah kecepatan pengiriman data menjadi berkurang karena adanya tambahan kode. Sistem ini biasanya digunakan untuk mengenali nasabah dan melindungi informasi finansial nasabah.

2) Sistem *Firewall*

Firewall merupakan sistem yang digunakan untuk mencegah pihak-pihak yang tidak diizinkan untuk memasuki daerah yang dilindungi dalam unit pusat kerja perusahaan. *Firewall* berusaha untuk mencegah pihak-pihak yang mencoba masuk tanpa izin dengan cara melipatgandakan dan mempersulit hambatan-hambatan yang ada. Namun, yang perlu diingatkan adalah bahwa sistem *firewall* ini tidak dapat mencegah masuknya virus atau gangguan yang berasal dari dalam perusahaan itu sendiri.

f. Resiko Spesifik untuk *Internet Banking*

Internet banking memiliki kekhususan tersendiri sehingga ada beberapa risiko yang sifatnya sangat spesifik untuk *internet banking*, diantaranya adalah:

1) *Technology Risk*

Risiko teknologi yang berhubungan dengan kehandalan dan sistem keamanan. Kecanggihan *software* dan *hardware* sangat menentukan besar kecilnya risiko teknologi yang dihadapi oleh bank penyelenggara jasa *internet banking*.

2) *Reputational Risk*

Reputational risk berkaitan erat dengan *corporate image* dari bank itu sendiri. Nama baik bank penyelenggara *internet banking* menjadi jaminan utama dalam pelayanan jasa *internet banking*. Kegagalan atau tidak berfungsinya sistem, teknologi maupun aplikasi yang dipakai dalam *internet banking* dapat membuat nasabah menjadi *reluctant* atau enggan untuk melakukan transaksi perbankan melalui *internet*.

3) *Outsourcing Risk*

Dalam prakteknya hampir semua bank yang menyelenggarakan pelayanan transaksi melalui *internet* menggunakan jasa pihak ketiga sebagai *internet service provider* (ISP) ataupun sebagai data operator dalam pengoperasian dan pemeliharaan data. Di satu sisi bank dapat menghemat biaya yang cukup signifikan dengan melakukan *outsourcing* tetapi di sisi lain ada risiko yang mungkin timbul dengan

adanya *outsourcing* tersebut antara lain ditutupnya ISP tersebut secara tiba-tiba karena kesulitan keuangan, kurang terjaminnya kerahasiaan data karena ISP tersebut mudah dibobol oleh *hacker*, kurangnya kapabilitas ISP, dll.

4) *Legal Risk*

Masalah hukum dalam *internet banking* dalam beberapa hal masih banyak yang belum jelas dan belum diatur secara *eksplisit*. Hal ini dapat menimbulkan potensi masalah yang besar di bidang hukum perdata atau pidana apabila di kemudian hari terjadi sengketa atau perselisihan yang menyangkut transaksi-transaksi perbankan yang dilakukan melalui *internet*. Selain itu *cross border issues* dalam transaksi *internet banking* sedikit banyak juga berkaitan dengan aspek hukum yang belum jelas.

5) *Transaction Risk*

Resiko transaksi merupakan risiko saat ini dan di masa mendatang sebagai akibat dari kecurangan, kesalahan, dan ketidakmampuan menyalurkan produk dan jasa, memelihara posisi yang kompetitif, dan mengelola informasi. Risiko transaksi terdapat pada setiap pemrosesan transaksi, pengembangan sistem, sistem perhitungan, kompleksitas, produk dan jasa, serta *internal control*. Risiko transaksi yang tinggi dapat terkandung pada produk *internet banking*, khususnya jika tidak direncanakan, diimplementasikan, dan dipantau dengan tepat.

g. Prinsip-prinsip dalam Pengaturan *Internet Banking*

Pengaturan *internet banking* di Indonesia bersifat longgar dan *technology neutral* agar tidak menghambat proses inovasi layanan perbankan melalui *internet banking*, bahkan diharapkan dapat mendorong pengembangannya di masa datang. Prasyarat yang perlu dipenuhi bank dalam menyelenggarakan pelayanan *internet banking* merupakan persyaratan minimum yang harus dipenuhi bank untuk memastikan bank telah menerapkan prinsip-prinsip *prudential banking operation, risk management*, dan perlindungan terhadap nasabah dan bank itu sendiri

Keberadaan praktik *internet banking* yang tidak terlepas dari berbagai risiko telah menjadi dasar bagi Bank Indonesia untuk membuat pengaturan yang bersifat *prudential* dan menganut prinsip *self regulatory banking*. Pada dasarnya pengaturan yang dibuat harus memperhatikan dan mengakomodasikan beberapa aspek penting, antara lain:

1) *Bank regulatory focus* bukan *technology focus*

Ketergantungan *internet banking* dengan teknologi sangat besar sekali bahkan unsur teknologi tersebut sangat dominan dalam *internet banking*. Oleh karena itu pengaturan *internet banking* ke depan akan lebih terfokus pada tujuan operasional perbankan dalam penyelenggaraan *internet banking* (*bank regulatory focus*). Perkembangan teknologi dan inovasinya dapat berubah tanpa mengenal batas waktu sehingga pengaturan yang bersifat *technology*

focus tidak akan mampu menampung perubahan-perubahan yang terjadi.

2) *The same protection level*

Praktek *internet banking* masih merupakan sesuatu yang baru di Indonesia mengingat masih terbatasnya jumlah bank penyedia jasa *internet banking*. Perkembangan *internet banking* ke depan selain dipengaruhi oleh faktor teknologi dan inovasi juga sangat dipengaruhi oleh unsur kepercayaan dari nasabah. Kepercayaan dari nasabah menyangkut transaksi di *internet* harus dijamin bahwa transaksi *internet banking* memberikan tingkat perlindungan yang seoptimal mungkin. Untuk itu pengaturan *internet banking* ke depan harus mampu menjamin kepentingan nasabah baik itu keamanan dalam bertransaksi ataupun kerahasiaan data nasabah.

- 3) Peraturan tidak menghambat pertumbuhan dan inovasi jasa pelayanan keuangan melalui internet dan justru sebaliknya harus mampu meningkatkan manfaatnya.
- 4) Harus memberi jaminan proteksi yang optimal terhadap nasabah maupun bank itu sendiri. Jaminan tersebut dimulai sejak transaksi dilakukan sampai selesainya transaksi tersebut.
- 5) Perhatian juga harus diarahkan pada aspek-aspek yang bersifat internasional, misalnya *home country supervision, cross border issue*, dan sebagainya.

Agar penyelenggaraan *internet banking* dapat memenuhi standar keamanan yang memadai dan memberikan perlindungan yang maksimum terhadap nasabah serta bank itu sendiri, maka sekurang-kurangnya pengaturan *internet banking* antara lain mencakup:

- 1) Perijinan
- 2) *Prudential Management:*
 - a) Sistem
 - b) Prosedur
 - c) Nama *Domain*
 - d) *Security*
 - e) *Internal Control*

h. Perlindungan Nasabah

Perlindungan nasabah sangat penting untuk menimbulkan kepercayaan dan kenyamanan nasabah untuk melakukan transaksi melalui *internet banking*. Karena *technology risk* dalam *internet banking* sangat tinggi, ada kemungkinan nasabah menderita kerugian karena datanya disadap oleh *hacker/cracker* atau memasuki *website* yang memiliki nama *domain* yang hampir sama. Untuk itu terdapat beberapa hal penting yang perlu diterapkan bank dalam rangka melakukan perlindungan terhadap nasabahnya, diantaranya:

- 1) *Client Charter:* yang memuat pernyataan dan komitmen bank untuk melaksanakan operasional *internet banking* yang aman, menjaga *privacy* atas informasi nasabah, memberikan pelayanan yang andal

dan berkualitas, transparansi produk dan jasa serta respon segera atas pertanyaan dan keluhan nasabah.

- 2) Kerahasiaan Data Nasabah (*Privacy Policy*): *privacy* atas informasi personal nasabah merupakan elemen penting dari kepercayaan dan keyakinan masyarakat atas sistem perbankan di Indonesia, untuk itu perbankan Indonesia diharapkan menyusun dan menerapkan kebijakan serta langkah-langkah nyata untuk menjaga dan menghargai *privacy* atas informasi personal nasabah dan mengungkapkan kebijakan tersebut secara terbuka kepada publik.
- 3) *Test and Trial Drive*: dalam rangka meningkatkan pemahaman nasabah dalam menggunakan layanan *internet banking*, bank dapat memberikan panduan penggunaan serta pelatihan (*test and trial drive*) bagi nasabah dalam menggunakan fitur dan fungsi yang dapat diperoleh nasabah di kantor bank atau pada *website* bank dalam bentuk *frequently asked question*, demo program, dll.
- 4) *Customer Support Service*: bank wajib menyediakan jasa layanan nasabah (*customer support service*) 24 jam yang dapat dihubungi melalui telepon, *electronic mail*, atau media lainnya untuk menjawab pertanyaan nasabah serta membantu para nasabah yang mengalami kesulitan dalam pengoperasian *internet banking*. Selain itu bank harus memiliki dan menginformasikan tentang prosedur pengajuan komplain nasabah, misalnya berupa kesanggupan bank untuk

melakukan audit trail dalam rangka pembuktian terbalik jika terjadi *dispute* antara bank dan nasabah mengenai suatu transaksi.

- 5) Sosialisasi: bank perlu mengambil langkah proaktif untuk memberikan pendidikan secara berkesinambungan dan menjelaskan kepada nasabah mengenai hak dan kewajiban mereka dan bagaimana mereka wajib menjaga kerahasiaan data-data mereka dalam melakukan kegiatan/transaksi di *internet*. Setiap terjadi perubahan sistem terutama yang terkait dengan keamanan (*security*), integritas data (*integrity*), dan keotentikan (*authentication*), kepada nasabah perlu diberikan informasi yang memadai agar mereka dapat menggunakan sistem tersebut. Sebelum menawarkan produk/jasa internet banking kepada nasabah, bank harus membuat suatu Pedoman Penggunaan *Internet Banking* bagi nasabahnya.

Client Charter dan *Privacy Policy* harus ditampilkan pada *website* bank. Perlu disampaikan juga pada website bank tentang *internet banking* yang memuat risiko-risiko yang timbul akibat transaksi *internet banking*.

Selain itu, pada *website* perlu ditampilkan pula Terminologi dan Persyaratan (*term and conditions*) dalam bahasa yang sederhana, jelas, dan mudah dipahami yang harus dipahami serta perlu disetujui nasabah sebelum dapat melakukan transaksi melalui *internet banking*. Jika *term and conditions* disampaikan dalam Bahasa Inggris harus disertai pula dengan Bahasa Indonesia. Perubahan atas pasal-pasal dalam *term and*

conditons perlu disampaikan kepada nasabah dengan diberi pendanaan khusus agar menarik perhatian, seperti warna yang berbeda, *highlight*,dll.

i. Pengaturan *Internet Banking* di Indonesia

Dalam Surat Edaran Bank Indonesia No. 9/30/DPNP tentang Penerapan Manajemen Resiko dalam Penggunaan Teknologi Informasi oleh Bank Umum tanggal 12 Desember 2007, dapat dilihat bahwa pelaksanaan teknologi sistem informasi diserahkan kepada masing-masing bank. Bank Indonesia hanya memberikan pedoman sehingga di dalam pelaksanaannya tidak merugikan nasabah dan bank itu sendiri.

Sementara itu, dalam Lampiran Surat Edaran Bank Indonesia No. 9/30/DPNP tentang Pedoman Penerapan Manajemen Resiko dalam Penggunaan Teknologi Informasi oleh Bank Umum disebutkan bahwa perkembangan pesat Teknologi Informasi (TI) dan globalisasi mendukung Bank untuk meningkatkan pelayanan kepada nasabah secara aman, nyaman, dan efektif, diantaranya melalui media elektronik atau dikenal dengan *e-banking*. Melalui *e-banking*, nasabah bank pada umumnya dapat mengakses produk dan jasa perbankan dengan menggunakan berbagai peralatan elektronik (*intelligent electronic device*), seperti *personal computer* (PC), *personal digital assistant* (PDA), anjungan tunai mandiri (ATM), kios, atau telephone.

Electronic banking adalah layanan yang memungkinkan nasabah bank untuk memperoleh informasi, melakukan komunikasi, dan melakukan transaksi perbankan melalui media elektronik, seperti

Automatic Teller Machine (ATM), phone banking, electronic fund transfer (EFT), Electronic Data Capture (EDC)/Point Of Sales (POS), internet banking dan mobile banking.

B. Penelitian yang Relevan

Penelitian yang telah ada sebelumnya dan sesuai dengan penelitian ini adalah sebagai berikut:

1. Penelitian yang dilakukan oleh Nidia Putri Harry (2015) dalam skripsinya yang berjudul “Perlindungan Hukum Terhadap Nasabah Bank Pengguna Fasilitas Internet Banking Atas Tejadinya *Cyber Crime* (Studi Kasus: *Bussines Banking Center Mandiri Padang”). Penelitian ini bertujuan untuk mengetahui perlindungan hukum terhadap nasabah bank dalam pengguna fasilitas *internet banking* atas terjadinya *cybercrime* di *Bussines Banking Center* Mandiri Padang dan untuk mengetahui kendala dari *Bussines Banking Center* Mandiri Padang dalam melakukan perlindungan hukum terhadap nasabah bank pengguna fasilitas *internet banking* atas terjadinya *cybercrime*. Hasil penelitian ini menunjukkan bahwa perlindungan hukum atas data pribadi dan dana nasabah dalam penyelenggaraan *internet banking* dengan pendekatan pengaturan secara *internal* dari penyelenggara *internet banking* itu sendiri. Sedangkan kendala yang ditemukan dalam rangka memberikan perlindungan hukum terhadap nasabah pengguna fasilitas *internet banking* di *Business Centre* Mandiri Padang adalah kemungkinan terjadinya penyalahgunaan atau kejahatan jasa layanan elektronik oleh pihak yang tidak bertanggung jawab, koneksi jaringan yang terkadang tidak stabil,*

sumber daya manusia kurang mendukung, tidak adanya undang-undang yang mengatur secara khusus mengenai kejahatan *cyber crime* dalam dunia perbankan khususnya pengguna *internet banking*. Persamaan dalam penelitian ini yaitu sama-sama mengkaji tentang kejahatan *cyber* yang menyerang nasabah pengguna *internet banking*. Sedangkan perbedaan dalam penelitian ini yaitu teknik pengambilan datanya. Dalam penelitian ini menggunakan metode kualitatif dengan menggunakan wawancara langsung saja tanpa angket atau kuesioner.

2. Penelitian yang dilakukan Hatialum Rehulina BR Silalahi (2012) dalam skripsinya yang berjudul “ Analisis Yuridis Kejahatan *Cyber Crime* dalam Pembobolan Mesin ATM Bank”. Penelitian ini bertujuan untuk mengetahui bagaimana akibat hukum terhadap pembobolan mesin ATM bank dalam Hukum Pidana serta bagaimana perlindungan hukum terhadap nasabah korban pembobolan ATM Bank. Hasil penelitian dapat disimpulkan bahwa pembobolan ATM Bank yang dilakukan oleh pelaku dapat di hukum dalam hukum pidana atau dalam KUHP serta dapat diberat dengan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Persamaan dalam penelitian ini yaitu sama-sama mengkaji tentang kejahatan *cyber* yang menyerang nasabah. Sedangkan perbedaan dalam penelitian ini yaitu teknik pengambilan datanya. Dalam penelitian ini menggunakan metode kualitatif dengan menggunakan wawancara langsung saja tanpa angket atau kuesioner. Selain itu juga dalam penelitian ini yang dikaji hanya kasus pembobolan ATM saja sedangkan penelitian yang akan

saya lakukan lebih terfokus pada kejahatan *cyber* di semua produk *internet banking*.

3. Penelitian yang dilakukan oleh Antonius Maria Laot Kian (2015) dalam jurnalnya berjudul “ Tindak Pidana *Credit/Debit Card Fraud* dan Penerapan Sanksi Pidananya dalam Hukum Pidana Indonesia”. Penelitian ini bertujuan untuk mengetahui pengaturan hukum dan penerapan sanksi pidana terhadap tindak pidana *credit/debit card fraud* di Indonesia. Hasil penelitian menunjukkan pengaturan dan sanksi pidana terhadap tindak pidana *credit/debit card fraud* di Indonesia masih tergolong minim. Pertama, belum diakomodasinya ketentuan yang secara langsung mengatur mengenai *computer related fraud*. Kedua, belum diaturnya sanksi pidana berbentuk tindakan yang bersifat *restitutif* bagi pelakunya. Persamaan dalam penelitian ini yaitu sama-sama mengkaji tentang kejahatan *cyber* yang menyerang nasabah pengguna *internet banking*. Sedangkan perbedaan dalam penelitian ini yaitu teknik pengambilan datanya. Dalam penelitian ini menggunakan tipe penelitian hukum normatif. Penelitian ini berpijak pada konstruksi norma hukum positif.
4. Penelitian yang dilakukan oleh Dwi Ayu Astrini (2015) dalam jurnalnya yang berjudul “Perlindungan Hukum terhadap Nasabah Bank Pengguna *Internet Banking* dari Ancaman *Cyber Crime*”. Penelitian ini bertujuan untuk mengetahui bagaimana peraturan perundang-undangan yang melindungi nasabah bak pengguna *internet banking* dari ancaman *cyber crime*, dan bagaimana mekanisme perlindungan dan tanggungjawab yang

diberikan pihak bank terhadap nasabah yang mengalami masalah dalam pengguna *internet banking*. Persamaan dalam penelitian ini yaitu sama-sama mengkaji tentang kejahatan *cyber* yang menyerang nasabah pengguna *internet banking*. Sedangkan perbedaan dalam penelitian ini yaitu teknik pengambilan datanya. Dalam penelitian ini menggunakan metode penulisan kepustakaan yang bersifat yuridis normatif dan data yang diperoleh data sekunder.

C. Kerangka Berfikir

1. Pengaruh Penggunaan *Internet Banking* terhadap Terjadinya *Cyber Crime*

Pada konteks penggunaan *internet banking* dapat diartikan bahwa penggunaan *internet banking* dapat meningkatkan kinerja bagi nasabah yang menggunakannya. Seseorang akan menggunakan *internet banking* apabila orang tersebut mengetahui bahwa *internet banking* dapat memberikan manfaat dalam melaksanakan tugas atau pekerjaannya. Oleh karena itu semakin nasabah merasakan manfaat *internet banking* dalam hal meningkatkan kinerja, efektivitas dan manfaat sistem lainnya maka nasabah akan semakin sering menggunakan *internet banking*. Tetapi dibalik kemudahan itu muncul suatu jenis kejahatan baru dalam perkembangan teknologi yang berbasis internet. Dengan diadopsinya inovasi baru berupa *internet banking* inilah, dapat memunculkan adanya jenis kejahatan melalui internet yang dikenal dengan istilah *cyber crime*. Banyaknya hacker yang mulai bermunculan di dunia digital seperti ini membuat masyarakat pengguna fasilitas internet harus ekstra hati-hati

dalam melindungi data pribadinya. Ini merupakan salah satu tugas penting yang harus dilakukan pihak bank untuk memberikan fitur keamanan yang memadai bagi nasabahnya.

2. Pengaruh Aspek *Client Charter* terhadap *Cyber Crime*

Untuk dapat mempertahankan hubungan jangka panjang dengan para nasabahnya, pihak bank perlu memberikan perlindungan nasabah agar nasabah selalu merasa aman dan nyaman dalam menggunakan fasilitas *internet banking*. Aspek perlindungan nasabah berupa *client charter* yang disediakan bank menerapkan konsep bahwa bank akan selalu memberikan pelayanan yang andal, berkualitas, dan menjamin bahwa operasional *internet banking* yang digunakan itu aman. Sehingga dapat meminimalisir bahkan mencegah terjadinya cyber crime dalam penggunaan *internet banking*. Oleh karena itu semakin percaya nasabah akan sistem keamanan dari layanan *internet banking* terhadap terjadinya *cyber crime* akan membuat semakin seringnya nasabah dalam menggunakan fasilitas ini.

3. Pengaruh Aspek Kerahasiaan Data Nasabah terhadap *Cyber Crime*

Untuk dapat mempertahankan hubungan jangka panjang dengan para nasabahnya, pihak bank perlu memberikan perlindungan nasabah agar nasabah selalu merasa aman dan nyaman dalam menggunakan fasilitas *internet banking*. Aspek perlindungan nasabah berupa kerahasiaan data nasabah yang disediakan bank menerapkan konsep bahwa bank akan selalu menjaga dan menghargai privasi atas informasi personal nasabah. Sehingga nasabah akan selalu merasa aman ketika melakukan transaksi

dalam bentuk apapun. Dengan adanya perlindungan ini diharapkan dapat memiminimalisir dan mencegah terjadinya *cyber crime*. Oleh karena itu semakin percaya nasabah akan sistem keamanan dari layanan *internet banking* terhadap terjadinya *cyber crime* akan membuat semakin seringnya nasabah dalam menggunakan fasilitas ini.

4. Pengaruh Aspek *Test and Trial Drive* terhadap *Cyber Crime*

Untuk dapat mempertahankan hubungan jangka panjang dengan para nasabahnya, pihak bank perlu memberikan perlindungan nasabah agar nasabah selalu merasa aman dan nyaman dalam menggunakan fasilitas *internet banking*. Aspek perlindungan nasabah berupa *test and trial drive* yang disediakan bank menerapkan konsep bahwa bank akan memberikan panduan atau simulasi penggunaan serta pelatihan menggunakan fungsi dan fitur layanan kepada para nasabah baru pengguna *internet banking* khususnya. Dengan adanya aspek ini nasabah tidak perlu khawatir apabila tidak bisa menggunakan fasilitas *internet banking* ini dengan baik. Karena dengan layanan ini nasabah mendapatkan informasi penggunaan *internet banking* yang baik dan benar sesuai dengan prosedur yang ada. Simulasi penggunaan fitur atau fungsi ini disediakan dalam aplikasi maupun *website* bank penyedia *internet banking*. Dengan adanya perlindungan ini diharapkan dapat memiminimalisir dan mencegah terjadinya *cyber crime*. Oleh karena itu semakin percaya nasabah akan sistem keamanan dari layanan *internet banking* terhadap terjadinya *cyber crime* akan membuat semakin seringnya nasabah dalam menggunakan fasilitas ini.

5. Pengaruh Aspek *Customer Support Service* terhadap *Cyber Crime*

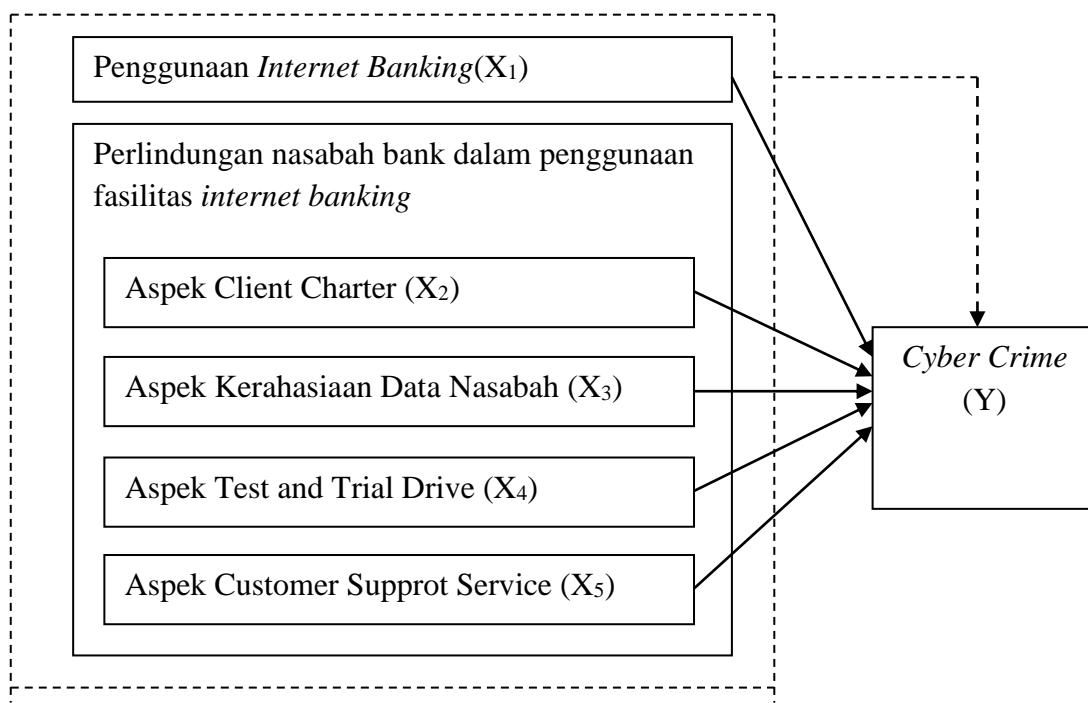
Untuk dapat mempertahankan hubungan jangka panjang dengan para nasabahnya, pihak bank perlu memberikan perlindungan nasabah agar nasabah selalu merasa aman dan nyaman dalam menggunakan fasilitas *internet banking*. Aspek perlindungan nasabah berupa *customer support service* yang disediakan bank menerapkan konsep bahwa bank memberikan layanan 24 jam bagi nasabah yang mengalami kesulitan, serta pihak bank wajib memberikan solusi terbaik bagi semua keluhan nasabah yang disampaikan baik secara langsung maupun melalui media seperti telepon atau *electronic mail (e-mail)*. Dengan adanya perlindungan ini diharapkan dapat memiminimalisir dan mencegah terjadinya *cyber crime*. Oleh karena itu semakin percaya nasabah akan sistem keamanan dari layanan *internet banking* terhadap terjadinya *cyber crime* akan membuat semakin seringnya nasabah dalam menggunakan fasilitas ini.

6. Pengaruh Penggunaan *Internet Banking* dan Perlindungan Nasabah terhadap *Cyber Crime*

Penggunaan *internet banking* yang semakin memudahkan nasabah dalam melakukan segala bentuk aktivitas dan transaksi perbankan membuat fasilitas *internet banking* menjadi fasilitas yang banyak diminati nasabahnya. Seiring dengan banyaknya nasabah yang menggunakan fasilitas ini, akan lebih baik lagi bila bank memberikan perlindungan bagi nasabahnya untuk melindungi seluruh data pribadi nasabah agar nasabah selalu merasa aman dan nyaman selama menggunakan fasilitas ini.

Perkembangan zaman yang menuntut adanya inovasi khususnya di bidang perbankan membuat bank harus ekstra dalam melakukan perlindungan bagi nasabahnya mengingat *internet banking* ini sangat rawan sekali terhadap terjadinya kejadian dunia maya atau kejadian *cyber* atau lebih sering dikenal dengan sebutan *cyber crime*. Banyaknya kejadian seperti *hacking*, *cracking*, maupun *carding* membuat nasabah merasa risau dan gelisah akan keamanan data pribadinya. Oleh karenanya bank wajib memberikan fitur-fitur keamanan yang memadai dan mampu menjamin segala transaksi yang dilakukan nasabah itu aman.

D. Paradigma Penelitian



Gambar 3. Paradigma Penelitian

Keterangan:

X₁, X₂, X₃, X₄, X₅ = Variabel independen

Y = Variabel dependen

- = Pengaruh masing-masing variabel
- - - → = Pengaruh variabel secara simultan

E. Hipotesis Penelitian

Berdasarkan rumusan masalah, tujuan penelitian, landasan teori, dan kerangka berfikir penelitian, maka hipotesis yang diajukan dalam penelitian ini adalah:

H1 : Penggunaan *internet banking* berpengaruh secara signifikan terhadap *cyber crime*.

H2 : *Client Charter* berpengaruh secara signifikan terhadap *cyber crime*.

H3 : Kerahasiaan data nasabah berpengaruh secara signifikan terhadap *cyber crime*.

H4 : *Test and trial drive* berpengaruh secara signifikan terhadap *cyber crime*.

H5 : *Customer support service* berpengaruh secara signifikan terhadap *cyber crime*.

H6 : Penggunaan *internet banking* dan perlindungan nasabah dilihat dari aspek *client charter*, kerahasiaan data nasabah, *test and trial drive*, dan *customer support service* berpengaruh secara signifikan terhadap *cyber crime*.

BAB III

METODE PENELITIAN

A. Desain Penelitian

Dalam penelitian ini menggunakan metode penelitian deskriptif dengan pendekatan kuantitatif. Metode kuantitatif adalah pendekatan ilmiah terhadap pengambilan keputusan manajerial ekonomi. Pendekatan ini berangkat dari data yang kemudian diproses dan dimanipulasi menjadi informasi yang berharga bagi pengambilan keputusan (Kuncoro Mudrajad, 2007:2).

Jenis data yang digunakan dalam penelitian ini yaitu terdiri dari data primer dan data sekunder. Data primer adalah data yang diambil langsung dari objek penelitian, yaitu menggunakan kuisioner. Sedangkan data sekunder adalah data yang diperoleh dari dokumen-dokumen dari bank dan juga sumber-sumber lain yang berhubungan dengan penelitian ini.

B. Tempat dan Waktu Penelitian

Penelitian dilaksanakan di D.I. Yogyakarta. Pelaksanaan penelitian akan dilaksanakan bulan Maret 2018 sampai dengan Mei 2018 dengan pertimbangan untuk mendapatkan responden yang lebih tepat.

C. Populasi dan Sampel Penelitian

1. Populasi

Populasi adalah wilayah generalisasi yang terdiri atas: obyek/subyek yang mempunyai kualitas dan karakteristik tertentu yang ditetapkan oleh peneliti untuk dipelajari dan kemudian ditarik kesimpulannya (Sugiyono,

2012: 61). Populasi dalam penelitian ini yaitu pengguna *internet banking* di D.I. Yogyakarta.

2. Sampel

Sampel adalah bagian dari jumlah dan karakteristik yang dimiliki oleh populasi (Sugiyono, 2012: 62). Teknik pengambilan sampel dalam penelitian ini menggunakan teknik *insidental sampling*. Menurut Sugiyono (2012) *insidental sampling* adalah teknik penentuan sampel berdasarkan kebetulan, yaitu siapa saja yang secara kebetulan/insidental bertemu dengan peneliti dapat digunakan sebagai sampel, bila dipandang orang yang kebetulan ditemui itu cocok sebagai sumber data.

Menurut Roscoe (1975) dalam Uma Sekaran (2006) memberikan acuan umum untuk menentukan ukuran sampel yaitu apabila dalam penelitian multivariate (termasuk analisis regresi berganda), ukuran sampel sebaiknya 10 kali lebih besar dari jumlah variabel dalam penelitian. Dalam penelitian ini, penulis mengambil keputusan untuk mencari jumlah sampel dengan cara 12 dikali banyaknya variabel yaitu 6 sehingga sampel yang digunakan sebanyak 72 responden.

D. Definisi Operasional Variabel

1. *Cyber Crime*(Y)

a. *Cyber Crime* pernyataan yang memuat tentang kejahatan *cyber* yang pernah dialami oleh nasabah serta penanggulangannya dan juga pencegahan atau tindakan yang dilakukan oleh bank kepada nasabah yang belum pernah mengalami *cyber crime*. Variabel ini akan diukur

melalui sepuluh pernyataan. Setiap item diukur dengan menggunakan Skala Likert mulai dari 1 untuk Sangat Tidak Setuju sampai 5 untuk Sangat Setuju.

2. Penggunaan *Internet Banking*(X1)

Penggunaan internet banking adalah kondisi nyata nasabah yang menggunakan internet banking yang dikonseptkan dalam bentuk pengukuran terhadap frekuensi penggunaan transaksi yang dilakukan oleh nasabah. Variabel ini akan diukur melalui sepuluh pernyataan. Setiap item akan diukur dengan menggunakan Skala Likert mulai dari 1 untuk Sangat Tidak Setuju sampai 5 untuk Sangat Setuju.

2. Perlindungan Nasabah

Hal-hal penting yang perlu diterapkan bank dalam rangka melakukan perlindungan terhadap nasabahnya, yaitu:

b. *Client charter* (X2) : yang memuat pernyataan dan komitmen bank untuk melaksanakan operasional *internet banking* yang aman, menjaga *privacy* atas informasi nasabah, memberikan pelayanan yang andal dan berkualitas, transparansi produk dan jasa serta respon segera atas pertanyaan dan keluhan nasabah. Variabel ini akan diukur melalui sepuluh pernyataan. Setiap item diukur dengan menggunakan Skala Likert mulai dari 1 untuk Sangat Tidak Setuju sampai 5 untuk Sangat Setuju.

c. Kerahasiaan data nasabah (X3) : *privacy* atas informasi personal nasabah merupakan elemen penting dari kepercayaan dan keyakinan masyarakat

atas sistem perbankan di Indonesia, untuk itu perbankan Indonesia diharapkan menyusun dan menerapkan kebijakan serta langkah-langkah nyata untuk menjaga dan menghargai *privacy* atas informasi personal nasabah dan mengungkapkan kebijakan tersebut secara terbuka kepada publik. Variabel ini akan diukur melalui sepuluh pernyataan. Setiap item diukur dengan menggunakan Skala Likert mulai dari 1 untuk Sangat Tidak Setuju sampai 5 untuk Sangat Setuju.

- d. *Test and trial drive* (X4) : dalam rangka meningkatkan pemahaman nasabah dalam menggunakan layanan *internet banking*, bank dapat memberikan panduan penggunaan serta pelatihan (*test and trial drive*) bagi nasabah dalam menggunakan fitur dan fungsi yang dapat diperoleh nasabah di kantor bank atau pada *website* bank dalam bentuk *frequently asked question*, demo program. Variabel ini akan diukur melalui sepuluh pernyataan. Setiap item diukur dengan menggunakan Skala Likert mulai dari 1 untuk Sangat Tidak Setuju sampai 5 untuk Sangat Setuju.
- e. *Customer support service* (X5) : bank wajib menyediakan jasa layanan nasabah (*customer support service*) 24 jam yang dapat dihubungi melalui telepon, *electronic mail*, atau media lainnya untuk menjawab pertanyaan nasabah serta membantu para nasabah yang mengalami kesulitan dalam pengoperasian *internet banking*. Selain itu bank harus memiliki dan menginformasikan tentang prosedur pengajuan komplain nasabah, misalnya berupa kesanggupan bank untuk melakukan audit trail dalam rangka pembuktian terbalik jika terjadi *dispute* antara bank dan nasabah

mengenai suatu transaksi. Variabel ini akan diukur melalui sepuluh pernyataan. Setiap item diukur dengan menggunakan Skala Likert mulai dari 1 untuk Sangat Tidak Setuju sampai 5 untuk Sangat Setuju.

E. Teknik dan Instrumen Pengumpulan Data

1. Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan yaitu menggunakan teknik wawancara dan kuesioner atau angket. Wawancara adalah cara memperoleh informasi dengan bertanya langsung pada yang diwawancarai. Hasil wawancara ditentukan oleh beberapa faktor yang berinteraksi dan memengaruhi arus informasi (Syamsudin, 2007: 108). Teknik kuesioner adalah bentuk alat pengumpulan data dalam bentuk pertanyaan-pertanyaan. Diharapkan dengan menyebarkan daftar pertanyaan kepada responden, peneliti dapat menghimpun data yang relevan dengan tujuan penelitian memiliki tingkat reliabilitas dan validitas yang tinggi (Muhamad, 2008: 151).

Jenis kuesioner atau angket yang digunakan adalah angket tertutup. Angket tertutup yaitu angket yang disajikan dalam bentuk sedemikian rupa sehingga responden diminta untuk memilih satu jawaban yang sesuai dengan karakteristik dirinya dengan cara memberi tanda (x) atau *checklist* (✓) (Riduwan, 2007: 27). Skala pengukuran yang digunakan yaitu skala likert. Skala likert adalah skala yang digunakan untuk mengukur sikap, pendapat, dan persepsi seseorang atau sekelompok tentang kejadian dan gejala sosial (Riduwan, 2007: 12). Pemberian bobot skor diukur dengan skala Likert dengan keterangan sebagai berikut:

- a. Skor 5 untuk jawaban Sangat Setuju (SS)
- b. Skor 4 untuk jawaban Setuju (S)
- c. Skor 3 untuk jawaban Kurang Setuju (KS)
- d. Skor 2 untuk jawaban Tidak Setuju (TS)
- e. Skor 1 untuk jawaban Sangat Tidak Setuju (STS)

2. Instrumen Pegumpulan Data

Penelitian ini menggunakan instrumen berupa lembar kuesioner atau angket. Adapun langkah-langkah penyusunan instrumen adalah menjabarkan variabel menjadi sub variabel/dimensi, kemudian membuat kisi-kisi instrumen dari masing-masing variabel dalam penelitian ini, sebagai berikut.

Tabel 2. Kisi-kisi Kuesioner

No.	Variabel	Sub Variabel	Indikator	Nomor Item
1.	Perlindungan Nasabah	1.1.Penggunaan <i>Internet Banking</i>	<ul style="list-style-type: none"> a. Transaksi nasabah pengguna <i>internet banking</i> b. Penggunaan fasilitas <i>internet banking</i> 	1,2 3,4,5,6,7,8 9,10
		1.2. <i>Client Charter</i>	<ul style="list-style-type: none"> a. Pengendalian dalam melindungi nasabah b. Jaminan keamanan nasabah c. Privatisasi data nasabah d. Kepercayaan nasabah pada fasilitas <i>internet banking</i>. 	11,12 13,14,15,16 17 18,19,20
		1.3.Kerahasiaan Data	a. Kepercayaan nasabah terhadap	21

		Nasabah	<ul style="list-style-type: none"> b. bank b. Keamanan data c. Kerahasiaan data nasabah 	22,23 24,25,26,27 28,29,30
		1.4. <i>Test and Trial Drive</i>	<ul style="list-style-type: none"> a. Penyediaan situs informasi pada website b. Layanan website 	31,32,33 34,35,36,37 38,39,40
		1.5. <i>Customer Support Service</i>	<ul style="list-style-type: none"> a. Kemampuan customer service b. Pelayanan kepada nasabah c. Kesediaan layanan 	41,42 43,44,45,46 47 48,49,50
2.	<i>Cyber Crime</i>	2.1. Terjadinya Kejahatan Cyber	<ul style="list-style-type: none"> a. Terjadinya cyber crime pada nasabah b. Bentuk ganti rugi dari bank c. Kepercayaan nasabah d. Tindak lanjut pihak bank e. Perlindungan dari kejahatan cyber f. Peraturan yang berlaku 	1,2 3 4 5 6,7,8 9,10

F. Validitas dan Reliabilitas Instrumen

Kuesioner yang nantinya akan disebar kepada responden harus diuji terlebih dahulu validitas dan reliabilitasnya. Uji coba instrumen tersebut dilakukan untuk mengetahui apakah layak atau tidak instrumen tersebut digunakan dalam penelitian.

1. Uji Validitas

Uji validitas digunakan untuk mengukur sah/valid atau tidaknya suatu kuesioner. Kuesioner dikatakan valid jika pertanyaan pada kuesioner

mampu mengungkapkan sesuatu yang akan diukur oleh kuesioner tersebut (Danang Sunyoto, 2011: 72). Teknik yang digunakan untuk uji validitas pada penelitian ini adalah teknik korelasi *product moment* dari *pearson* (Suharsimi, 2009: 171)

Setelah r hitung ditemukan, nilai r hitung tersebut kemudian dikonsultasikan dengan tabel untuk mengetahui butir yang valid dan tidak valid. Dengan pedoman bila r hitung $\geq r$ tabel pada signifikansi 5% maka butir item dianggap valid, sedangkan bila r hitung $< r$ tabel maka item itu dianggap tidak valid. Butir yang digunakan dalam pengumpulan data adalah butir yang valid (Imam Ghazali, 2006: 49)

Dalam penelitian ini, peneliti menggunakan uji coba validitas terpakai. Dalam uji coba terpakai peneliti langsung menyajikannya pada subjek penelitian, lalu peneliti menganalisis validitasnya sehingga diketahui item valid dan tidak valid. Seleksi item dilakukan dengan melakukan pengujian validitas terhadap semua item di setiap variabel

Untuk mendapatkan data ini, penulis menggunakan uji validitas terpakai. Uji validitas ini digunakan untuk menguji validitas seluruh sampel penelitian yaitu sebanyak 72 responden dengan memberikan sebanyak 60 butir pertanyaan. Apabila hasil uji validitas $> 0,235$, maka pernyataan dianggap valid dan dapat digunakan dalam penelitian selanjutnya.

Tabel 3. Hasil Uji Validitas

No.	Variabel	Jumlah Item Awal	Jumlah Butir Valid	Jumlah Butir Tidak Valid	Jumlah Akhir
1.	Penggunaan <i>Internet Banking</i>	10	10	0	10
2.	<i>Client Charter</i>	10	10	0	10
3.	Kerahasiaan Data Nasabah	10	10	0	10
4.	<i>Test and Trial Drive</i>	10	10	0	10
5.	<i>Customer Support Service</i>	10	10	0	10
6.	<i>Cyber Crime</i>	10	10	0	10
	Jumlah	60	60	0	60

Sumber: data primer yang diolah

2. Uji Reliabilitas

Pengertian reliabilitas adalah alat untuk mengukur suatu kuesioner yang merupakan indikator dari variabel atau konstruk. Butir pertanyaan dikatakan reliabel atau andal apabila jawaban seseorang terhadap pertanyaan adalah konsisten (Danang Sunyoto, 2011: 67-68). Dengan menggunakan instrumen yang valid dan reliabel dalam pengumpulan data, maka diharapkan hasil penelitian akan menjadi valid dan reliabel. Jadi instrumen yang valid dan reliabel merupakan syarat untuk mendapatkan hasil penelitian yang valid dan reliabel (Sugiyono, 2012: 348).

“Instrumen yang reliabel adalah instrumen yang bila digunakan beberapa kali untuk mengukur objek yang sama, akan menghasilkan data yang sama”. Uji reliabilitas pada penelitian ini dihitung dengan menggunakan rumus *Alpha Cronbach*. Perhitungan estimasi reliabilitas skala diterima, jika hasil perhitungan r_{hitung} lebih besar $r_{tabel} 5\%$. Menurut

Sugiyono (2013 ; 257) tingkatan hasil estimasi reliabilitas adalah sebagai berikut:

Tabel 4. Tingkatan Hasil Estimasi Reliabilitas

Besarnya nilai r	Interpretasi
Antara 0,800 sampai dengan 1,000	Sangat Tinggi
Antara 0,600 sampai dengan 0,799	Tinggi
Antara 0,400 sampai dengan 0,599	Sedang
Antara 0,200 sampai dengan 0,399	Rendah
Antara 0,000 sampai dengan 0,199	Sangat Rendah

Sumber: Sugiyono (2013 ; 257)

Dalam penelitian ini, instrumen yang diuji dengan menggunakan estimasi reliabilitas tersebut hanyalah kuesioner dengan jenis kuesioner tertutup saja, yaitu untuk variabel Penggunaan *Internet Banking*, *Client Charter*, Kerahasiaan Data Nasabah, *Test and Trial Drive*, *Customer Support Service*, dan *Cyber Crime*. Hal ini dikarenakan jenis kuesioner terbuka tidak perlu menggunakan estimasi reliabilitas.

Berdasarkan hasil olah data uji coba angket menggunakan SPSS 17 di bawah ini estimasi reliabilitas angket menunjukkan interpretasi Tinggi dan Sangat Tinggi. Hal itu berarti bahwa tingkat reliabilitas instrumen yang diuji masing-masing dinyatakan reibel untuk digunakan dalam penelitian ini.

Tabel 5. Hasil Uji Reliabilitas

Variabel	Koefisien Reliabilitas	Interpretasi
Penggunaan <i>Internet Banking</i> (X1)	0,910	Sangat Tinggi
<i>Client Charter</i> (X2)	0,848	Sangat Tinggi
Kerahasiaan Data Nasabah (X3)	0,780	Tinggi
<i>Test and Trial Drive</i> (X4)	0,875	Sangat Tinggi
<i>Customer Support Service</i> (X5)	0,873	Sangat Tinggi
<i>Cyber Crime</i> (Y)	0,865	Sangat Tinggi

Sumber: data primer yang diolah

G. Teknik Analisis Data

Alat analisis yang digunakan yaitu alat analisis deskriptif kuantitatif.

Pengolahan data dilakukan secara manual dan menggunakan komputer dengan program Microsoft Office Excel dan Program SPSS.

1. Analisis Deskriptif

Analisis deskriptif dalam penelitian ini digunakan untuk menganalisis data yang diperoleh dari responden melalui angket yang telah diisi oleh responden selama penelitian berlangsung yang kemudian disajikan dalam bentuk deskripsi data dari masing-masing variabel (variabel bebas dan variabel terikat). Deskripsi data yang digunakan meliputi:

a. Mean, Median, Modus, dan Standar Deviasi

Mean atau nilai rata-rata adalah jumlah total dibagi jumlah individu. Median adalah suatu nilai yang membatasi 50% dari frekuensi distribusi atas dan 50% dari distribusi frekuensi bawah. Modus adalah nilai variabel yang mempunyai frekuensi terbanyak dalam distribusi. Penentuan mean, median, dan modus dilakukan dengan menggunakan software SPSS.

b. Distribusi Frekuensi

Dalam membuat tabel distribusi frekuensi dilakukan langkah-langkah sebagai berikut:

1) Menentukan Kelas Interval

Untuk menentukannya menggunakan rumus Stuges sebagai berikut:

$$K = 1 + 3,3 \log n$$

Keterangan:

K = Jumlah Kelas

n = Jumlah data atau responden

Log = Logaritma

2) Menghitung Rentang Kelas

Untuk mengitung rentang data digunakan rumus sebagai berikut:

$$\text{Rentang data} = \text{nilai maksimum} - \text{nilai minimum}$$

3) Menentukan Panjang Kelas

Untuk menunjukkan panjang kelas digunakan rumus sebagai berikut:

$$\text{Panjang kelas} = \text{Rentang kelas} / \text{Jumlah kelas}$$

c. Kategorisasi

Deskripsi selanjutnya adalah melakukan pengkategorian terhadap nilai masing-masing indikator. Dari nilai tersebut dibagi menjadi 3 kategori berdasarkan *mean* ideal (M_i) dan standar deviasi ideal (S_{di}). Rumus untuk mencari *mean* ideal (M_i) dan standar deviasi ideal (S_{di}) adalah sebagai berikut:

$$\text{Mean Ideal } (M_i) = \frac{1}{2} (\text{nilai maksimum} + \text{nilai minimum})$$

$$\text{Standar Deviasi Ideal } (S_{di}) = \frac{1}{6} (\text{nilai maksimum} - \text{nilai minimum})$$

Sedangkan untuk mencari kategori indikator adalah sebagai berikut:

Tinggi = $\{M_i + 1 (S_{di})\}$

Sedang = $< \{M_i - 1 (S_{di})\}$ s/d $\{M_i + 1 (S_{di})\}$

Rendah = $< \{M_i - 1 (S_{di})\}$

2. Uji Prasyarat Analisis

Setelah melakukan tahap-tahap di atas, data yang telah dikumpulkan harus diuji dahulu untuk dapat dianalisis. Pengujian prasyarat dilakukan sebelum pengujian hipotesis, antara lain:

a. Uji Linearitas

Uji linearitas bertujuan untuk mengetahui apakah variabel independen (x) dan variabel dependen (y) mempunyai hubungan linear atau tidak dengan melihat apakah data yang dimiliki sesuai dengan garis linier atau tidak. Analisis regresi linear dapat dilakukan apabila asumsi linieritas terpenuhi. Linearitas dapat diketahui melalui uji linearitas tabel Anova dengan mencari nilai *Deviation from Linearity* dari uji F linear.

Hipotesis yang diajukan adalah sebagai berikut:

H_0 : Model regresi linear

H_1 : Model regresi tidak linear

Jika *Deviation from Linearity* menunjukkan nilai $sig > 0,05$ maka H_0 diterima. Jika *Deviation from Linearity* menunjukkan nilai $sig < 0,05$ maka H_0 ditolak.

b. Multikolinieritas

Uji ini sebagai syarat digunakannya analisis regresi ganda untuk mengkaji terjadi atau tidaknya multikolinieritas antar variabel independen. Multikolinieritas adalah korelasi antara variabel independen satu dengan yang lain. “Model regresi yang baik seharusnya tidak terjadi korelasi di antara variabel independen”. Untuk menguji multikolinearitas

dilakukan dengan melihat nilai *Variance Inflation Factor* (VIF). Nilai *Variance Inflation Factor* (VIF) adalah faktor inflasi penyimpangan baku kuadrat (Sunyoto, 2007: 89). Dikatakan tidak terjadi multikolenieritas jika koefisien korelasi antarvariabel bebas memiliki nilai VIF kurang dari 4 (Muhsan Ali, 2015: 39).

c. Heteroskedastisitas

Uji heteroskedastisitas bertujuan untuk menguji apakah dalam model regresi terjadi ketidaksamaan *variance* dari residual satu pengamatan ke pengamatan lain. Jika residualnya mempunyai varians yang sama, disebut terjadi homoskedastisitas, dan jika variansnya tidak sama/berbeda disebut terjadi heteroskedastisitas (Danang Sunyono, 2011: 82). Salah satu uji statistik yang dapat digunakan untuk mendeteksi ada tidaknya heteroskedastisitas adalah Uji *Glejser* yang mengusulkan untuk meregres nilai absolut residual terhadap variabel independen. Jika variabel independen secara signifikan secara statistik tidak mempengaruhi variabel dependen, maka tidak terdapat indikasi terjadi heteroskedastisitas. Hal ini dapat dilihat apabila dari probabilitas signifikansinya di atas tingkat kepercayaan 5%.

d. Uji Normalitas

Uji normalitas data digunakan untuk menguji apakah dalam model regresi, variabel penganggu masih memiliki distribusi normal atau tidak. Banyak cara yang dapat digunakan untuk melakukan pengujian

terhadap normal tidaknya penyebaran data, salah satunya adalah dengan menggunakan Metode Kolmogorov-Smirnov.

3. Regresi Linier Berganda

Analisis regresi ganda digunakan oleh peneliti, bila peneliti bermaksud meramalkan bagaimana keadaan (naik turunnya) variabel dependen (kriteria), bila dua atau lebih variabel independen sebagai faktor prediktor dimanipulasi (dinaik turunkan nilainya). Jadi analisis regresi ganda akan dilakukan bila jumlah variabel independennya minimal 2. Model analisis regresi berganda dengan menggunakan persamaan model sebagai berikut:

$$KC = \beta_0 + \beta_1 PI + \beta_2 CC + \beta_3 RD + \beta_4 TT + \beta_5 CS + Et$$

Keterangan:

KC : Kejahatan *Cyber*

PI : Aspek Penggunaan *Internet Banking*

CC : Aspek *Client Charter*

RD : Aspek Kerahasiaan Data Nasabah

TT : Aspek *Test and Trial Drive*

CS : Aspek *Customer Support Service*

β_0 : Konstanta

β_{1-6} : Koefisien Regresi

Et : Error Term

4. Uji Kelayakan Model

a. Koefisien Determinasi (R^2)

Koefisien Determinasi (R^2) merupakan nilai yang menyatakan proporsi atau presentase dari total varian variabel dependen (Y) yang dapat dijelaskan oleh variabel (X_1 , X_2 , X_3 , dan X_4) secara bersama-sama. Nilai koefisien R^2 berada diantara 0 dan 1 ($0 \leq R^2 \leq 1$). Apabila nilai 1, garis regresi dapat menjelaskan 100% varian pada variabel Y. Sebaliknya apabila bernilai 0, model regresi tersebut tidak dapat menjelaskan variansi sedikitpun pada variabel Y. Kelemahan mendasar penggunaan koefisien determinasi adalah bias terhadap jumlah variabel independen yang dimasukkan ke dalam model. Setiap tambahan satu variabel independen, maka R^2 pasti meningkat tidak peduli apakah variabel tersebut berpengaruh secara signifikan terhadap variabel dependen atau tidak.

b. Uji Kelayakan Model dengan Uji F

Uji F merupakan tahapan awal mengidentifikasi model regresi yang diestimasi layak atau tidak. Layak disini maksudnya adalah model yang diestimasi layak digunakan untuk menjelaskan pengaruh variabel-variabel bebas terhadap variabel terikat. Apabila nilai prop F (output SPSS ditunjukkan pada kolom sig) hitung lebih kecil dari tingkat kesalahan/error 0,05 maka dapat dikatakan bahwa model regresi diestimasi layak, dan sebaliknya.

c. Menguji Signifikansi dengan Uji t

Uji t pada dasarnya menunjukkan seberapa jauh pengaruh satu variabel bebas secara individual dalam menerangkan variasi variabel dependen. Setelah ditemukan nilai t hitung, nilai t hitung dibandingkan dengan t tabel dengan taraf signifikansi 5%. Apabila nilai t hitung lebih tinggi dibandingkan nilai t tabel, maka variabel memiliki pengaruh yang signifikan (Imam Ghozali, 2006: 89).

5. Mencari Sumbangan Relatif (SR) dan Sumbangan Efektif (SE)

a. Sumbangan Relatif

Sumbangan relatif adalah persentase perbandingan antara realitivitas yang diberikan satu variabel bebas kepada variabel terikat dengan variabel-variabel bebas yang lain. Sumbangan relatif ini digunakan untuk mengetahui seberapa besar sumbangan masing-masing prediktor dalam perbandingan terhadap nilai kriterium untuk keperluan prediksi. Rumus yang digunakan adalah sebagai berikut:

$$SR(X)\% = \frac{SE(X)\%}{R^2}$$

Keterangan:

$SR\%X_1$: Sumbangan relatif X_1

$SR\%X_2$: Sumbangan relatif X_2

$SR\%X_3$: Sumbangan relatif X_3

$SR\%X_4$: Sumbangan relatif X_4

$SR\%X_5$: Sumbangan relatif X_5

b. Sumbangan Efektif (SE)

Sumbangan efektif digunakan untuk mengetahui besarnya sumbangan secara efektif setiap prediktor terhadap kriterium dengan tetap memperhitungkan variabel bebas lain yang tidak diteliti. Rumus yang digunakan untuk menghitung besarnya sumbangan efektif adalah:

$$\mathbf{SE\,(X)\% = Beta_x \times r_{xy} \times 100\%}$$

Keterangan:

SE% : Sumbangan efektif dari suatu prediktor

r_{xy} : Koefisien korelasi

SE%X₁ : Sumbangan efektif X₁

SE%X₂ : Sumbangan efektif X₂

SE%X₃ : Sumbangan efektif X₃

SE%X₄ : Sumbangan efektif X₄

SE%X₅ : Sumbangan efektif X₅

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

A. Hasil Penelitian

1. Deskripsi Data

Data yang digunakan dalam penelitian ini didapatkan dengan menyebar kuesioner *online* dan *offline* kepada para responden. Jumlah kuesioner disebar kepada para responden sebanyak 72 buah sesuai dengan jumlah sampel penelitian. Dari seluruh kuesioner yang kembali, peneliti mengolah dan manganalisis data. Responden dalam penelitian ini adalah pengguna internet banking di Daerah Istimewa Yogyakarta.

a. Deskripsi Responden Berdasarkan Jenis Kelamin

Deskripsi data responden berdasarkan jenis kelamin dapat dilihat pada tabel 6 berikut:

Tabel 6. Demografi Responden Berdasarkan Jenis Kelamin

Jenis Kelamin	Frekuensi	Presentase (%)
Laki-laki	26	36.11
Perempuan	46	63.89
Jumlah	72	100.00

Sumber: data primer yang diolah

Data tersebut menunjukkan persentase responden laki-laki yang memakai *internet banking* sejumlah 26 orang (36,11%), sedangkan responden perempuan yang memakai *internet banking* sejumlah 46 orang (63,89%).

b. Deskripsi Responden Berdasarkan Usia

Deskripsi data responden berdasarkan usia dapat dilihat pada tabel 7 berikut:

Tabel 7. Demografi Responden Berdasarkan Usia

Usia	Frekuensi	Presentase (%)
17 – 19	5	6,94
20 – 22	54	75,00
23 – 25	9	12,50
26 – 28	2	2,78
29 – 31	0	0,00
32 – 34	0	0,00
35 – 37	0	0,00
38 – 40	1	1,39
41 – 43	1	1,39
Jumlah	72	100,00

Sumber: data primer yang diolah

Data tersebut menunjukkan jumlah persentase umur yang memakai *internet banking*. Dari data responden tersebut dapat dilihat bahwa sebagian besar responden yang memakai *internet banking* masuk usia 20-22 tahun sejumlah 54 orang (75%), kemudian disusul usia 17-19 tahun sejumlah 5 orang (6,94%), kemudian usia 26-28 tahun sejumlah 2 orang (2,78%), kemudian usia 38-40 tahun dan 41-43 tahun yang sama-sama berjumlah 1 orang (1,39%), dan terakhir masuk pada usia 29-37 tahun yang sama-sama berjumlah 0 orang (0,00%).

c. Deskripsi Responden Berdasarkan Lama Menggunakan *Internet Banking*

Deskripsi data responden berdasarkan lama menggunakan *internet banking* dapat dilihat pada tabel 8 berikut:

Tabel 8. Demografi Responden Berdasarkan Lama Penggunaan *Internet Banking*

Lama Penggunaan <i>Internet Banking</i>	Jumlah	Presentase (%)
< 1 tahun	25	34.72
1 – 2 tahun	28	38.89
3 – 4 tahun	13	18.06
4 – 5 tahun	1	1.39
>5 tahun	5	6.94
Total		100.00

Sumber: data primer yang diolah

Data tersebut menunjukkan bahwa sebagian besar responden menggunakan *internet banking* antara 1-2 tahun sejumlah 28 orang (38,89%), kemudian responden yang menggunakan *internet banking* kurang dari 1 tahun sejumlah 25 orang (34,72%), kemudian responden yang menggunakan *internet banking* antara 3-4 tahun sejumlah 13 orang (18,06%), kemudian yang menggunakan *internet banking* lebih dari 5 tahun sejumlah 5 orang (6,94%), dan responden yang menggunakan *internet banking* antara 4-5 tahun sejumlah 1 orang (1,39%).

d. Deskripsi Responden Berdasarkan Intensitas Penggunaan *Internet Banking* per Bulan

Deskripsi data responden berdasarkan intensitas penggunaannya per bulan dapat dilihat pada tabel 9 berikut:

Tabel 9. Demografi Responden Berdasarkan Intensitas Penggunaan *Internet Banking* per Bulan

Intensitas Penggunaan per Bulan	Frekuensi	Presentase (%)
Tidak Pernah	6	8.33
1 – 3 kali	32	44.44
4 – 6 kali	14	19.44
7 – 10 kali	4	5.56
>10 kali	16	22.22
Total	72	100.00

Sumber: data primer yang diolah

Data tersebut menunjukkan intensitas sebagian besar responden yang menggunakan *internet banking* per bulannya paling sering menggunakan dengan intensitas 1-3 kali sejumlah 32 orang (44,44%), kemudian dengan intensitas lebih dari 10 kali sejumlah 16 orang (22,22%), kemudian dengan intensitas 4-6 kali sejumlah 14 orang (19,44%), kemudian dengan intensitas tidak pernah menggunakan *internet banking* tiap bulannya sejumlah 6 orang (8,33%), dan dengan intensitas 7-10 kali sejumlah 4 orang (5,56%).

2. Deskripsi Variabel Penelitian

Analisis deskriptif dalam penelitian ini meliputi *mean*, *median*, *modus*, tabel frekuensi, dan tabel frekuensi responden menurut kategori yang penentuannya menggunakan bantuan program SPSS 17.0. Penentuan tabel distribusi frekuensi dilakukan dengan menentukan kelas interval, menghitung rentang data, dan menentukan panjang kelas.

Untuk mendeskripsikan dan menguji pengaruh variabel independen terhadap variabel dependen dalam penelitian ini, maka akan disajikan deskripsi data dari tiap-tiap variabel berdasarkan data yang diperoleh di

lapangan. Deskripsi data masing-masing variabel secara rinci dapat dilihat dalam uraian berikut ini:

a. Variabel Terjadinya *Cyber Crime*

Data variabel Terjadinya *Cyber Crime* diperoleh dari angket yang terdiri dari 10 butir pertanyaan. Angket tersebut disusun menggunakan Skala Likert yang dimodifikasi yang terdiri dari 5 alternatif jawaban. Skor yang diberikan maksimal 5 dan minimal 1, sehingga diperoleh skor tertinggi ideal 60 dan skor terendah ideal 10. Berdasarkan data penelitian yang diolah menggunakan bantuan komputer program SPSS 17, variabel Terjadinya *Cyber Crime* memiliki skor tertinggi sebesar 48, skor terendah sebesar 10, *mean* sebesar 30,77, *median* sebesar 30, *modus* sebesar 29, dan standar deviasi sebesar 7,46.

Jumlah kelas interval setelah dihitung dengan rumus Sturges sebanyak 8 kelas dengan panjang kelas 5. Hasil perhitungan selengkapnya dapat dilihat pada lampiran halaman 163. Tabel distribusi frekuensi variabel *Cyber Crime* adalah sebagai berikut:

Tabel 10. Distribusi Frekuensi variabel *Cyber Crime*

No.	Interval	Frekuensi	Persen (%)	Persen Kumulatif (%)
1	10-14	1	1,39	1,39
2	15-19	2	2,78	4,17
3	20-24	10	13,89	18,06
4	25-29	20	27,78	45,83
5	30-34	21	29,17	75,00
6	35-39	7	9,72	84,72
7	40-44	6	8,33	93,06
8	45-49	5	6,94	100,00
Jumlah		72	100,00	

Sumber: data primer yang diolah

Tabel 10 menunjukkan bahwa frekuensi paling besar adalah 21 yaitu pada interval 30-34 dengan prosentase 29,17% sedangkan frekuensi paling rendah yaitu sebanyak 1 yang terdapat pada interval 10-14 dengan prosentase sebesar 1,39%. Distribusi kecenderungan data variabel *Cyber Crime* dapat dikategorikan dalam 3 kategori yaitu rendah, sedang, dan tinggi. Hasil perhitungan selengkapnya dapat dilihat pada lampiran halaman 151. Berikut tabel 11 mengenai distribusi kecenderungan data variabel *Cyber Crime*:

Tabel 11. Distribusi Kecenderungan Variabel *Cyber Crime*

No.	Kategori	Interval	Frekuensi	Frekuensi Relatif (%)
1	Tinggi	> 37	12	16,67
2	Sedang	23 s/d 37	52	72,22
3	Rendah	< 23	8	11,11
Total			72	100,00

Sumber: data primer yang diolah

Tabel 11 menunjukkan bahwa kategori tinggi sebanyak 12 responden (16,67%), kategori sedang 52 responden (72,22%), dan kategori rendah 8 responden (11,11%). Dari hasil tersebut dapat disimpulkan bahwa penilaian responden tentang variabel *Cyber Crime* adalah sedang karena mayoritas responden memberikan penilaian sedang. Hal tersebut digambarkan dalam Diagram Lingkaran Distribusi Frekuensi Kecenderungan Data Variabel *Cyber Crime* sebagai berikut:

b. Penggunaan *Internet Banking*

Data variabel Penggunaan *Internet Banking* diperoleh dari angket yang terdiri dari 10 butir pertanyaan. Angket tersebut disusun

menggunakan Skala Likert yang dimodifikasi yang terdiri dari 5 alternatif jawaban. Skor yang diberikan maksimal 5 dan minimal 1, sehingga diperoleh skor tertinggi ideal 60 dan skor terendah ideal 10. Berdasarkan data penelitian yang diolah menggunakan bantuan komputer program SPSS 17, variabel Penggunaan *Internet Banking* memiliki skor tertinggi sebesar 50, skor terendah sebesar 11, *mean* sebesar 37,80, *median* sebesar 39, *modus* sebesar 39, dan standar deviasi sebesar 6,67.

Jumlah kelas interval setelah dihitung dengan rumus Sturges sebanyak 8 kelas dengan panjang kelas 5. Berikut tabel 12 distribusi frekuensi variabel Penggunaan *Internet Banking* adalah sebagai berikut:

Tabel 12. Distribusi Frekuensi Variabel Penggunaan *Internet Banking*

No.	Interval	Frekuensi	Persen (%)	Persen Kumulatif (%)
1	11-15	1	1,39	1,39
2	16-20	1	1,39	2,78
3	21-25	1	1,39	4,17
4	26-30	5	6,94	11,11
5	31-35	11	15,28	26,39
6	36-40	29	40,28	66,67
7	41-45	18	25,00	91,67
8	46-50	6	8,33	100,00
Jumlah		72	100,00	

Sumber: data primer yang diolah

Tabel 12 menunjukkan bahwa frekuensi paling besar adalah 29 yaitu pada interval 36-40 dengan prosentase 40,28% sedangkan frekuensi paling rendah yaitu sebanyak 1 yang terdapat pada interval 11-15, 16-20, 21-25 dengan prosentase sebesar 1,39%. Distribusi kecenderungan data variabel Penggunaan *Internet Banking* dapat dikategorikan dalam 3

kategori yaitu rendah, sedang, dan tinggi. Hasil perhitungan selengkapnya dapat dilihat pada lampiran halaman 159. Berikut tabel 13 mengenai distribusi kecenderungan data variabel Penggunaan *Internet Banking*

Tabel 13. Distribusi Kecenderungan Variabel Penggunaan *Internet Banking*

No.	Kategori	Interval	Frekuensi	Frekuensi Relatif (%)
1	Tinggi	> 37	43	59,72
2	Sedang	23 s/d 37	27	37,50
3	Rendah	< 23	2	2,78
Total			72	100,00

Sumber: data primer yang diolah

Tabel 13 menunjukkan bahwa kategori tinggi sebanyak 43 responden (59,72%), kategori sedang 27 responden (37,50%), dan kategori rendah 2 responden (2,78%). Dari hasil tersebut dapat disimpulkan bahwa penilaian responden tentang variabel Penggunaan *Internet Banking* adalah tinggi karena mayoritas responden memberikan penilaian tinggi.

c. *Client Charter*

Data variabel *Client Charter* diperoleh dari angket yang terdiri dari 10 butir pertanyaan. Angket tersebut disusun menggunakan Skala Likert yang dimodifikasi yang terdiri dari 5 alternatif jawaban. Skor yang diberikan maksimal 5 dan minimal 1, sehingga diperoleh skor tertinggi ideal 60 dan skor terendah ideal 10. Berdasarkan data penelitian yang diolah menggunakan bantuan komputer program SPSS 17, variabel *Client Charter* memiliki skor tertinggi sebesar 50, skor terendah sebesar

31, *mean* sebesar 40,05, *median* sebesar 40, *modus* sebesar 40, dan standar deviasi sebesar 4,17.

Jumlah kelas interval setelah dihitung dengan rumus Sturges sebanyak 8 kelas dengan panjang kelas 3. Tabel distribusi frekuensi variabel *Client Charter* adalah sebagai berikut:

Tabel 14. Distribusi Frekuensi Variabel *Client Charter*

No.	Interval	Frekuensi	Persen (%)	Persen Kumulatif (%)
1	31-33	5	6,94	6,94
2	34-36	6	8,33	15,28
3	37-39	21	29,17	44,44
4	40-42	25	34,72	79,17
5	43-45	6	8,33	87,50
6	46-48	4	5,56	93,06
7	49-51	5	6,94	100,00
8	52-54	0	0,00	100,00
Jumlah		72	100,00	

Sumber: data primer yang diolah

Tabel 14 menunjukkan bahwa frekuensi paling besar adalah 25 yaitu pada interval 40-42 dengan prosentase 34,72% sedangkan frekuensi paling rendah yaitu sebanyak 0 yang terdapat pada interval 52-54 dengan prosentase sebesar 0,00%. Distribusi kecenderungan data variabel *Client Charter* dapat dikategorikan dalam 3 kategori yaitu rendah, sedang, dan tinggi. Berikut tabel 15 mengenai distribusi kecenderungan data variabel *Client Charter*:

Tabel 15. Distribusi Kecenderungan Variabel *Client Charter*

No.	Kategori	Interval	Frekuensi	Frekuensi Relatif (%)
1	Tinggi	> 37	56	77,78
2	Sedang	23 s/d 37	16	22,22
3	Rendah	< 23	0	0,00
Total			72	100,00

Sumber: data primer yang diolah

Tabel 15 menunjukkan bahwa kategori tinggi sebanyak 56 responden (77,78%), kategori sedang 16 responden (22,22%), dan kategori rendah 0 responden (0,00%). Dari hasil tersebut dapat disimpulkan bahwa penilaian responden tentang variabel *Client Charter* adalah tinggi karena mayoritas responden memberikan penilaian tinggi.

d. Kerahasiaan Data Nasabah

Data variabel Kerahasiaan Data Nasabah diperoleh dari angket yang terdiri dari 10 butir pertanyaan. Angket tersebut disusun menggunakan Skala Likert yang dimodifikasi yang terdiri dari 5 alternatif jawaban. Skor yang diberikan maksimal 5 dan minimal 1, sehingga diperoleh skor tertinggi ideal 60 dan skor terendah ideal 10. Berdasarkan data penelitian yang diolah menggunakan bantuan komputer program SPSS 17, variabel Kerahasiaan Data Nasabah memiliki skor tertinggi sebesar 50, skor terendah sebesar 30, *mean* sebesar 38,73, *median* sebesar 39, *modus* sebesar 39, dan standar deviasi sebesar 4,12.

Jumlah kelas interval setelah dihitung dengan rumus Sturges sebanyak 8 kelas dengan panjang kelas 3. Tabel distribusi frekuensi variabel Kerahasiaan Data Nasabah adalah sebagai berikut:

Tabel 16. Distribusi Frekuensi Kerahasiaan Data Nasabah

No.	Interval	Frekuensi	Persen (%)	Persen Kumulatif (%)
1	30-32	5	6,94	6,94
2	33-35	6	8,33	15,28
3	36-38	21	29,17	44,44
4	39-41	32	44,44	88,89
5	42-44	1	1,39	90,28
6	45-47	2	2,78	93,06
7	48-50	5	6,94	100,00
8	51-53	0	0,00	100,00
Jumlah		72	100,00	

Sumber: Data primer yang diolah

Tabel 16 menunjukkan bahwa frekuensi paling besar adalah 32 yaitu pada interval 39-41 dengan prosentase 44,44% sedangkan frekuensi paling rendah yaitu sebanyak 0 yang terdapat pada interval 51-53 dengan prosentase sebesar 0,00%. Distribusi kecenderungan data variabel Kerahasiaan Data Nasabah dapat dikategorikan dalam 3 kategori yaitu rendah, sedang, dan tinggi. Berikut tabel 17 mengenai distribusi kecenderungan data variabel Kerahasiaan Data Nasabah:

Tabel 17. Distribusi Kecenderungan Variabel Kerahasiaan Data Nasabah

No.	Kategori	Interval	Frekuensi	Frekuensi Relatif (%)
1.	Tinggi	> 37	45	62,50
2.	Sedang	23 s/d 37	27	37,50
3.	Rendah	< 23	0	0,00
Total			72	100,00

Sumber: data primer yang diolah

Tabel 17 menunjukkan bahwa kategori tinggi sebanyak 45 responden (62,50%), kategori sedang 27 responden (37,50%), dan kategori rendah 0 responden (0,00%). Dari hasil tersebut dapat disimpulkan bahwa

penilaian responden tentang variabel Kerahasiaan Data Nasabah adalah tinggi karena mayoritas responden memberikan penilaian tinggi.

e. *Test and Trial Drive*

Data variabel *Test and Trial Drive* diperoleh dari angket yang terdiri dari 10 butir pertanyaan. Angket tersebut disusun menggunakan Skala Likert yang dimodifikasi yang terdiri dari 5 alternatif jawaban. Skor yang diberikan maksimal 5 dan minimal 1, sehingga diperoleh skor tertinggi ideal 60 dan skor terendah ideal 10. Berdasarkan data penelitian yang diolah menggunakan bantuan komputer program SPSS 17, variabel *Test and Trial Drive* memiliki skor tertinggi sebesar 50, skor terendah sebesar 28, *mean* sebesar 38,43, *median* sebesar 38, *modus* sebesar 36, dan standar deviasi sebesar 5,12.

Jumlah kelas interval setelah dihitung dengan rumus Sturges sebanyak 8 kelas dengan panjang kelas 3. Tabel distribusi frekuensi variabel *Test and Trial Drive* adalah sebagai berikut:

Tabel 18. Distribusi Frekuensi Variabel Test and Trial Drive

No.	Interval	Frekuensi	Persen (%)	Persen Kumulatif (%)
1	28-30	5	6,94	6,94
2	31-33	8	11,11	18,06
3	34-36	15	20,83	38,89
4	37-39	19	26,39	65,28
5	40-42	10	13,89	79,17
6	43-45	10	13,89	93,06
7	46-48	3	4,17	97,22
8	49-51	2	2,78	100,00
Jumlah		72	100,00	

Sumber: data primer yang diolah

Tabel 18 menunjukkan bahwa frekuensi paling besar adalah 19 yaitu pada interval 37-39 dengan prosentase 26,39% sedangkan frekuensi paling rendah yaitu sebanyak 2 yang terdapat pada interval 49-51 dengan prosentase sebesar 2,78%. Distribusi kecenderungan data variabel *Test and Trial Drive* dapat dikategorikan dalam 3 kategori yaitu rendah, sedang, dan tinggi. Berikut tabel 19 mengenai distribusi kecenderungan data variabel *Test and Trial Drive*:

Tabel 19. Distribusi Kecenderungan Variabel Test and Trial Drive

No	Kategori	Interval	Frekuensi	Frekuensi Relatif (%)
1	Tinggi	> 37	40	55,56
2	Sedang	23 s/d 37	32	44,44
3	Rendah	< 23	0	0,00
Total			72	100,00

Sumber: data primer yang diolah

Tabel 19 menunjukkan bahwa kategori tinggi sebanyak 40 responden (55,56%), kategori sedang 32 responden (44,44%), dan kategori rendah 0 responden (0,00%). Dari hasil tersebut dapat disimpulkan bahwa penilaian responden tentang variabel *Tes and Trial Drive* adalah tinggi karena mayoritas responden memberikan penilaian tinggi.

f. *Customer Support Service*

Data variabel *Customer Support Service* diperoleh dari angket yang terdiri dari 10 butir pertanyaan. Angket tersebut disusun menggunakan Skala Likert yang dimodifikasi yang terdiri dari 5 alternatif jawaban. Skor yang diberikan maksimal 5 dan minimal 1, sehingga diperoleh skor tertinggi ideal 60 dan skor terendah ideal 10. Berdasarkan data penelitian

yang diolah menggunakan bantuan komputer program SPSS 17, variabel *Customer Support Service* memiliki skor tertinggi sebesar 50, skor terendah sebesar 29, *mean* sebesar 39,61, *median* sebesar 40, *modus* sebesar 40, dan standar deviasi sebesar 4,32.

Jumlah kelas interval setelah dihitung dengan rumus Sturges sebanyak 8 kelas dengan panjang kelas 3. Tabel distribusi frekuensi variabel *Customer Support Service* adalah sebagai berikut:

Tabel 20. Distribusi Frekuensi Variabel Customer Support Service

No	Interval	Frekuensi	Persen (%)	Persen Kumulatif (%)
1	29-31	3	4,17	4,17
2	32-34	5	6,94	11,11
3	35-37	11	15,28	26,39
4	38-40	32	44,44	70,83
5	41-43	9	12,50	83,33
6	44-46	7	9,72	93,06
7	47-49	2	2,78	95,83
8	50-52	3	4,17	100,00
Jumlah		72	100,00	

Sumber: data primer yang diolah

Tabel 20 menunjukkan bahwa frekuensi paling besar adalah 32 yaitu pada interval 38-40 dengan prosentase 44,44% sedangkan frekuensi paling rendah yaitu sebanyak 2 yang terdapat pada interval 47-49 dengan prosentase sebesar 2,78%. Distribusi kecenderungan data variabel *Customer Support Service* dapat dikategorikan dalam 3 kategori yaitu rendah, sedang, dan tinggi. Berikut tabel 21 mengenai distribusi kecenderungan data variabel *Customer Support Service*:

Tabel 21. Distribusi Kecenderungan Variabel Customer Support Service

No	Kategori	Interval	Frekuensi	Frekuensi Relatif (%)
1	Tinggi	> 37	53	73,61
2	Sedang	23 s/d 37	19	26,39
3	Rendah	< 23	0	0,00
	Total		72	100,00

Sumber: data primer yang diolah

Tabel 21 menunjukkan bahwa kategori tinggi sebanyak 53 responden (73,61%), kategori sedang 19 responden (26,39%), dan kategori rendah 0 responden (0,00%). Dari hasil tersebut dapat disimpulkan bahwa penilaian responden tentang variabel *Customer Support Service* adalah tinggi karena mayoritas responden memberikan penilaian tinggi.

3. Uji Prasyarat Analisis Data

a. Uji Normalitas Data

Uji normalitas data dilakukan untuk mengetahui apakah dalam model regresi, variabel pengganggu atau residual mempunyai distribusi normal atau tidak. Uji normalitas pada penelitian ini menggunakan *I-Sample Kolmogorov-Smirnov* dalam SPSS 17.0.

Tabel 22. Hasil Uji Normalitas

Asymp.Sig	Keterangan
0,975	Berdistribusi normal

Sumber: data primer yang diolah

Berdasarkan hasil uji normalitas di atas, karena nilai *Asymp.Sig.* di atas 0,05 maka dapat disimpulkan bahwa data berdistribusi normal.

b. Uji Linearitas

Uji linearitas digunakan untuk mengetahui model yang digunakan linear atau tidak. Berdasarkan output SPSS 17.0 hasil perhitungan uji linearitas dapat dilihat pada tabel 23:

Tabel 23. Hasil Uji Linearitas

Hubungan	<i>Deviation From Linearity</i>	Kriteria
X ₁ – Y	0,674	Linear
X ₂ – Y	0,154	Linear
X ₃ – Y	0,202	Linear
X ₄ – Y	0,401	Linear
X ₅ – Y	0,311	Linear

Sumber: data primer yang diolah

Hasil uji linearitas di atas menunjukkan bahwa *Deviation From Linearity* untuk semua model memiliki nilai signifikansi di atas 0,05. Maka dapat disimpulkan bahwa model tersebut linear dan dapat digunakan untuk uji regresi linear.

c. Uji Asumsi Klasik

1) Uji Multikolinearitas

Uji multikolinearitas bertujuan untuk menguji apakah dalam model regresi ditemukan adanya korelasi antar variabel bebas (independen).

Hasil perhitungan uji multikolinearitas dapat dilihat pada tabel 24:

Tabel 24. Hasil Uji Multikolinearitas

Variabel	Perhitungan	
	<i>Tolerance</i>	VIF
Penggunaan Internet Banking	0,795	1,259
Client Charter	0,559	1,790
Kerahasiaan Data Nasabah	0,583	1,715
Test and Trial Drive	0,629	1,591
Customer Support Sevice	0,753	1,328

Sumber: data primer yang diolah

Karena nilai VIF <4 maka dapat disimpulkan bahwa tidak ada multikolinearitas dalam model regresi.

2) Uji Heteroskedastisitas

Uji heteroskedastisitas bertujuan untuk menguji apakah dalam model regresi terjadi ketidaksamaan *variance* dari residual satu pengamatan ke pengamatan yang lain. Jika variance dari residual satu pengamatan ke pengamatan lain tetap, maka disebut homokedastisitas, atau tidak terjadi heterokedastisitas. Penelitian ini menggunakan uji *Glejser* dalam SPSS 17.0. Hasil uji heterokedastisitas dengan uji *Glejser* dapat dijelaskan pada tabel 25:

Tabel 25. Hasil Uji Heteroskedastisitas

Variabel Bebas	Sig	Keterangan
Penggunaan IB (X_1)	0,972	Tidak Terjadi Heteroskedastisitas
Client Charter (X_2)	0,630	Tidak Terjadi Heteroskedastisitas
Kerahasiaan Data Nasabah (X_3)	0,625	Tidak Terjadi Heteroskedastisitas
Test and Trial Drive (X_4)	0,834	Tidak Terjadi Heteroskedastisitas
Customer Support Service (X_5)	0,808	Tidak Terjadi Heteroskedastisitas

Sumber: data primer yang diolah

Dari uji *Glejser* di atas menunjukkan bahwa tidak terjadi heterokedastisitas untuk semua variabel karena probabilitasnya di atas 5%.

4. Uji Hipotesis

a. Analisis Regresi Ganda

Uji regresi ganda digunakan untuk menguji hipotesis keenam yang dimaksudkan manganalisis pengaruh variabel independen (X_1 , X_2 , X_3 ,

X_4 , dan X_5) secara bersama-sama terhadap variabel dependen (Y).

Pengolahan data menggunakan SPSS 17.0.

Tabel 26. Hasil Uji Regresi Berganda

Variabel Independen	Koefisien Regresi	t hitung	Sig
Konstanta	-2,911	-0,304	0,762
Penggunaan IB (X_1)	0,281	2,124	0,037
<i>Client Charter</i> (X_2)	-0,591	-2,341	0,022
Kerahasiaan Data Nasabah (X_3)	0,630	2,518	0,014
<i>Test and Trial Drive</i> (X_4)	0,036	0,187	0,852
<i>Customer Support Service</i> (X_5)	0,528	2,514	0,014
F hitung		4,714	
F tabel		2,37	
R		0,513	
R ²		0,263	
Sig F		0,001	
Adjusted R Square		0,207	

Sumber: data primer yang diolah

Berdasarkan hasil perhitungan regresi linier berganda yang ditunjukkan tabel di atas, maka persamaan garis regresinya adalah seperti berikut:

$$Y = -2,911 + 0,281X_1 - 0,591X_2 + 0,630X_3 + 0,036X_4 + 0,528X_5$$

Nilai koefisien X_1 sebesar 0,281 yang berarti apabila Penggunaan *Internet Banking* meningkat 1 poin maka Terjadinya *Cyber Crime* akan naik sebesar 0,281 satuan dengan asumsi X_2 , X_3 , X_4 , dan X_5 tetap. Nilai koefisien X_2 sebesar -0,591 yang berarti apabila variabel *Client Charter* meningkat 1 poin maka Terjadinya *Cyber Crime* akan turun sebesar 0,591 dengan asumsi X_1 , X_3 , X_4 , dan X_5 tetap. Nilai koefisien X_3 sebesar 0,630 yang berarti apabila Kerahasiaan Data Nasabah meningkat 1 poin maka Terjadinya *Cyber Crime* akan naik sebesar 0,630 satuan dengan asumsi X_1 , X_2 , X_4 , dan X_5 tetap. Nilai koefisien X_4 sebesar

0,036 yang berarti apabila *Test and Trial Drive* meningkat 1 poin maka Terjadinya *Cyber Crime* akan naik sebesar 0,036 satuan dengan asumsi X1, X2, X3, dan X5 tetap. Nilai koefisien X5 sebesar 0,528 yang berarti apabila *Customer Support Service* meningkat 1 poin maka Terjadinya *Cyber Crime* akan naik sebesar 0,528 satuan dengan asumsi X1, X2, X3, dan X4 tetap.

b. Uji Parsial (t)

Uji t merupakan pengujian untuk menunjukkan pengaruh secara individu variabel bebas yang ada dalam model terhadap variabel terikat. Hal ini dimaksudkan untuk mengetahui seberapa jauh pengaruh satu variabel bebas dalam menjelaskan variabel terikat. Untuk menunjukkan pengaruh secara individu variabel bebas terhadap variabel terikat juga dapat dilihat pada nilai signifikansinya.

Berdasarkan hasil perhitungan parsial pengaruh Penggunaan *Internet Banking* terhadap *Cyber Crime* diperoleh nilai koefisien sebesar 0,281. Pada taraf signifikansi 5% dapat diketahui t_{hitung} sebesar 2,124 dengan nilai signifikansi 0,037 karena koefisien regresi mempunyai nilai positif dan signifikansi (p) < 0,05 maka hipotesis pertama yang berbunyi “Terdapat pengaruh positif Penggunaan *Internet Banking* terhadap *Cyber Crime*” diterima.

Hasil perhitungan secara parsial pengaruh *Client Charter* terhadap *Cyber Crime* diperoleh nilai koefisien regresi sebesar -0,591. Pada taraf signifikansi 5%, dapat diketahui t_{hitung} sebesar -2,341 dengan nilai

signifikansi sebesar 0,022, karena koefisien regresi mempunyai nilai negatif dan nilai signifikansi (p) < 0,05 maka hipotesis kedua yang berbunyi “Terdapat pengaruh *Client Charter* terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta” diterima.

Hasil perhitungan secara parsial pengaruh Kerahasiaan Data nasabah terhadap *Cyber Crime* diperoleh nilai koefisien regresi sebesar 0,630. Pada taraf signifikansi 5% dapat diketahui thitung sebesar 2,518 dengan nilai disgnifikasi sebesar 0,014, karena koefisien regresi mempunyai nilai positif dan nilai signifikansi (p) < 0,05 maka hipotesis ketiga yang berbunyi “Terdapat pengaruh positif Kerahasiaan Data Nasabah terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta” diterima.

Hasil perhitungan secara parsial pengaruh *Test and Trial Drive* terhadap *Cyber Crime* diperoleh nilai koefisien regresi sebesar 0,036. Pada taraf signifikansi 5%, dapat diketahui thitung sebesar 0,187 dengan nilai signifikansi sebesar 0,852, karena koefisien regresi mempunyai nilai positif dan signifikansi (p) > 0,05 maka hipotesis keempat yang berbunyi “Terdapat pengaruh *Test and Trial Drive* terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta” tidak diterima.

Hasil perhitungan pengaruh *Customer Support Service* terhadap *Cyber Crime* diperoleh nilai koefisien regresi sebesar 0,528. Pada taraf signifikansi 5%, dapat diketahui thitung sebesar 2,514 dengan nilai signifikansi sebesar 0,014, karena koefisien regresi mempunyai nilai

positif dan nilai signifikansi (p) < 0,05 maka hipotesis kelima yang berbunyi “Terdapat pengaruh *Customer Support Service* terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta” diterima.

c. Uji Simultan (F)

Uji simultan digunakan untuk mengetahui apakah variabel bebas yaitu Penggunaan *Internet Banking*, *Client Charter*, Kerahasiaan Data Nasabah, *Test and Trial Drive*, dan *Customer Support Service* secara bersama-sama berpengaruh terhadap variabel terikat yaitu *Cyber Crime*. Berdasarkan hasil perhitungan secara simultan pengaruh Penggunaan *Internet Banking*, *Client Charter*, Kerahasiaan Data Nasabah, *Test and Trial Drive*, dan *Customer Support Service* terhadap *Cyber Crime*, pada taraf signifikansi 5%, diperoleh nilai Fhitung sebesar 4,714 dengan nilai signifikansi F sebesar 0,001. Karena nilai signifikansi F < 0,05 maka hipotesis keenam yang berbunyi “Terdapat pengaruh Penggunaan *Internet Banking*, *Client Charter*, Kerahasiaan Data Nasabah, *Test and Trial Drive*, dan *Customer Support Service* secara bersama-sama terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta” diterima. Hal ini mengandung arti bahwa variabel Penggunaan *Internet Banking*, *Client Charter*, Kerahasiaan Data Nasabah, *Test and Trial Drive*, dan *Customer Support Service* mempunyai pengaruh yang signifikan terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta .

d. Koefisien Determinasi (R^2)

Koefisien determinasi digunakan untuk menunjukkan berapa besar prosentase variabel bebas (Penggunaan *Internet Banking*, *Client Charter*, Kerahasiaan Data Nasabah, *Test and Trial Drive*, dan *Customer Support Service*) secara bersama-sama menerangkan variansi variabel terikat (*Cyber Crime*). Hasil pengujian regresi ganda menunjukkan bahwa koefisien determinasi (R^2) sebesar 0,263 atau 26,3%. Nilai tersebut menunjukkan bahwa 26,3% terjadinya *Cyber Crime* dipengaruhi oleh Penggunaan *Internet Banking*, *Client Charter*, Kerahasiaan Data Nasabah, *Test and Trial Drive*, dan *Customer Support Service*. Sedangkan sisanya yaitu 73,3% dipengaruhi oleh variabel lain yang tidak diteliti dalam penelitian ini.

e. Sumbangan Relatif (SR) dan Sumbangan Efektif (SE)

Hasil analisis regresi ganda dapat diketahui besarnya sumbangan relatif dan sumbangan efektif (perhitungan pada lampiran halaman 165) masing-masing variabel independen terhadap variabel dependen dapat dilihat pada tabel sebagai berikut:

Tabel 27. Ringkasan Sumbangan Relatif dan Sumbangan Efektif

No.	Variabel	SR(%)	SE(%)
1.	Penggunaan <i>Internet Banking</i> (X1)	26,23	6,90
2.	<i>Client Charter</i> (X2)	13,30	3,50
3.	Kerahasiaan Data Nasabah (X3)	45,51	11,97
4.	<i>Test and Trial Drive</i> (X4)	2,43	0,64
5.	<i>Customer Support Service</i> (X5)	39,20	10,31
	Total	100,00	26,32

Sumber: data primer yang diolah

Berdasarkan tabel 24 dapat diketahui bahwa variabel Penggunaan *Internet Banking* memberikan sumbangan relatif sebesar 26,23% dan memberikan sumbangan efektif 6,90%. Variabel *Client Charter* memberikan sumbangan relatif sebesar 13,30% dan sumbangan efektif 3,50%. Variabel Kerahasiaan Data Nasabah memberikan sumbangan relatif sebesar 45,51% dan sumbangan efektif 11,97%. Variabel *Test and Trial Drive* memberikan sumbangan sebesar 2,43% dan sumbangan efektif 0,64%. Variabel *Customer Support Service* memberikan sumbangan relatif sebesar 39,20% dan sumbangan efektif 10,31%. Hal ini berarti bahwa variabel Kerahasiaan Data Nasabah yang memberikan sumbangan yang paling dominan. Berdasarkan tabel 24 dapat disimpulkan bahwa secara bersama-sama variabel Penggunaan *Internet Banking*, *Client Charter*, Kerahasiaan Data Nasabah, *Test and Trial Drive*, dan *Customer Supoort Service* memberikan sumbangan efektif sebesar 26,3% terhadap Cyber Crime dan 73,7% diberikan variabel-variabel diluar yang diteliti.

B. Pembahasan Hasil Penelitian

Penelitian ini bertujuan untuk menguji pengaruh antara Penggunaan *Internet Banking* (X1) dan Perlindungan Nasabah berupa *Client Charter* (X2), Kerahasiaan Data Nasabah(X3), *Test and Trial Drive* (X4), dan *Customer Support Service* (X5) terhadap *Cyber Crime* (Y) di Daerah Istimewa Yogyakarta. Berdasarkan hasil analisi, maka pembahasan tentang hasil penelitian adalah sebagai berikut:

1. Pengaruh Penggunaan *Internet Banking* terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta

Hasil dari penelitian mendukung hipotesis pertama (H1), bahwa variabel Penggunaan *Internet Banking* berpengaruh positif dan signifikan terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta. Hal ini ditunjukkan oleh nilai koefisien regresi sebesar 0,281. Koefisien regresi X1 sebesar 0,281 menyatakan bahwa setiap kenaikan Penggunaan *Internet Banking* sebesar 1 satuan akan menaikkan *Cyber Crime* sebesar 0,281 satuan. Hal ini berarti model tersebut adalah positif. Berdasarkan hasil analisis data diperoleh nilai t_{hitung} sebesar 2,124 yang nilainya di atas t_{tabel} sebesar 1,998. hasil ini menunjukkan bahwa t_{hitung} lebih besar dari t_{tabel} , hal ini berarti terdapat pengaruh positif Penggunaan *Internet Banking* terhadap *Cyber Crime* di DIY. Selain itu nilai probabilitas signifikansi Penggunaan *Internet Banking* sebesar 0,037 yang lebih kecil dari 0,05, maka dapat dinyatakan bahwa Penggunaan *Internet Banking* berpengaruh signifikan terhadap *Cyber Crime* di DIY sehingga hipotesis 1 didukung tingkat kepercayaan 95%.

Hasil tersebut memperkuat penelitian terbaru dari Kaspersky Lab. Dari data *Consumer Security Risks Survey* 2016 yang dilakukan oleh B2B International dan Kaspersky Lab, terungkap bila 5% pengguna global telah kehilangan uang secara *online* akibat penipuan *online*. Hal ini menunjukkan bahwa *new cyber crime* di perbankan juga sudah mulai muncul, tidak dengan teknik konvensional lagi tetapi dengan menggunakan aplikasi yang semakin maju juga, salah satunya melalui *internet banking* ini. *Trend*

menggunakan transaksi *banking* yang meningkat menimbulkan kejahatan *cyber crime* bidang ini juga meningkat hal ini dipengaruhi oleh meningkatnya penggunaan *mobile wallet*. Orang berbelanja dan melakukan pembayaran sudah tidak secara konvensional dengan datang ke kantor langsung, namun pembayaran dapat dilakukan secara *online banking* melalui *mobile banking*, *internet banking*, ATM, maupun toko swalayan yang menyediakan fasilitas pembayaran tersebut.

Hasil penelitian ini mengindikasi bahwa semakin banyak nasabah yang memanfaatkan fasilitas internet banking dapat memicu terjadinya *cyber crime*. Mengingat era sekarang ini sudah memasuki era *digital*, sehingga semakin banyak orang yang terampil dalam menggunakan teknologi dan tidak sedikit dari mereka yang justru menyalahgunakan teknologi tersebut.

2. Pengaruh *Client Charter* terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta

Hasil dari penelitian mendukung hipotesis kedua (H2), bahwa variabel *Client Charter* berpengaruh negatif dan signifikan terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta. Hal ini ditunjukkan oleh nilai koefisien regresi sebesar -0,591. Koefisien regresi X2 sebesar -0,591 menyatakan bahwa setiap penurunan *Client Charter* sebesar 1 satuan akan menaikkan *Cyber Crime* sebesar -0,591 satuan. Hal ini berarti model tersebut adalah negatif. Berdasarkan hasil analisis data diperoleh nilai t_{hitung} sebesar -2,341 yang nilainya di atas t_{tabel} sebesar 1,998. Hasil ini

menunjukkan bahwa t_{hitung} lebih besar dari t_{tabel} , hal ini berarti terdapat pengaruh negatif *Client Charter* terhadap *Cyber Crime* di DIY. Selain itu nilai probabilitas signifikansi *Client Charter* sebesar 0,022 yang lebih kecil dari 0,05, maka dapat dinyatakan bahwa *Client Charter* berpengaruh signifikan terhadap *Cyber Crime* di DIY sehingga hipotesis 2 didukung tingkat kepercayaan 95%.

Hasil penelitian ini mendukung pernyataan Perdana Menteri Margareth Thatcher di Inggris ketika pertama kali memperkenalkan istilah *Citizen Charter* yang dikenal juga dengan istilah *Client Charter* bahwa kontrak pelayanan merupakan pendekatan baru dalam pelayanan publik yang menempatkan pengguna layanan sebagai pusat perhatian atau unsur yang paling penting. Melalui *client charter* ini diharapkan akan dapat membentuk budaya melayani. Dalam konteks ini, kebutuhan dan kepentingan pengguna layanan menjadi pertimbangan utama dalam keseluruhan proses pemberian layanan.

Hasil ujicoba di beberapa daerah di Indonesia yang dijelaskan dalam jurnal Karjuni (2010) membuktikan bahwa penerapan *Client Charter* ini banyak manfaat yang akan dirasakan, baik oleh birokrasi, pengguna layanan, maupun stakeholders pengguna lainnya. Manfaat tersebut antara lain: Pertama, dapat memberikan kepastian pelayanan meliputi waktu, biaya, prosedur, dan cara pelayanan. Kedua, untuk memberikan informasi mengenai hak dan kewajiban pengguna layanan, penyedia layanan, dan stakeholder lainnya. Ketiga, untuk mempermudah proses kontrol

penyelenggaraan pelayanan. Keempat, membantu untuk memperbaiki kinerja pelayanan. Kelima, membantu untuk mengidentifikasi kebutuhan, harapan, dan aspirasi pengguna layanan.

Dari hasil penelitian menyatakan bahwa dengan adanya *Client Charter* ini diharapkan akan meminimalisir bahkan mencegah terjadinya *Cyber Crime* mengingat tujuan dari terbentuknya kontrak pelayanan atau *Client Charter* ini yaitu untuk membuat agar pelayanan publik menjadi lebih tanggap atau responsif, transparan, bertanggungjawab dan akuntabel. Sehingga *privacy* atas informasi nasabah *internet banking* aman dan terjaga dengan baik.

3. Pengaruh Kerahasiaan Data Nasabah terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta

Hasil dari penelitian mendukung hipotesis ketiga (H3), bahwa variabel Kerahasiaan Data Nasabah berpengaruh positif dan signifikan terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta. Hal ini ditunjukkan oleh nilai koefisien regresi sebesar 0,630. Koefisien regresi X3 sebesar 0,630 menyatakan bahwa setiap peningkatan Kerahasiaan Data Nasabah sebesar 1 satuan akan menaikkan *Cyber Crime* sebesar 0,630 satuan. Hal ini berarti model tersebut adalah positif. Berdasarkan hasil analisis data diperoleh nilai t_{hitung} sebesar 2,518 yang nilainya di atas t_{tabel} sebesar 1,998. Hasil ini menunjukkan bahwa t_{hitung} lebih besar dari t_{tabel} , hal ini berarti terdapat pengaruh positif Kerahasiaan Data Nasabah terhadap *Cyber Crime* di DIY. Selain itu nilai probabilitas signifikansi Kerahasiaan Data Nasabah

sebesar 0,014 yang lebih kecil dari 0,05, maka dapat dinyatakan bahwa Kerahasiaan Data Nasabah berpengaruh signifikan terhadap *Cyber Crime* di DIY sehingga hipotesis 3 didukung tingkat kepercayaan 95%.

Hasil penelitian menjelaskan bahwa semakin terjaga kerahasiaan nasabah akan mencegah terjadinya *cyber crime*. Sesuai dengan undang-undang tentang ketentuan rahasia bank di Indonesia yang diatur dalam UU No. 10 Tahun 1998 Pasal 40 ayat (1) menyebutkan bahwa bank wajib merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya. Rahasia bank yang dimaksud dengan segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpan dan simpanannya meliputi segala keterangan tentang orang dan badan yang memperoleh pemberian layanan dan jasa dalam lalu lintas uang.

Hasil penelitian ini juga didukung Muchammad Arya (2016) dalam jurnalnya tentang teori *absolut* rahasia bank yang menyatakan bahwa semua keterangan mengenai nasabah dan keuangannya yang tercatat di bank wajib dirahasiakan tanpa pengecualian dan pembatasan. Kerahasiaan mengenai nasabah dan keuangannya tidak boleh dibuka, dengan alasan apapun dan oleh siapapun. Kerahasiaan mengenai nasabah dan keuangannya tidak boleh dibuka dan bank harus bertanggung jawab atas segala akibat yang ditimbulkannya. Sedangkan menurut teori relatif, semua keterangan mengenai nasabah dan keuangannya yang tercatat di bank wajib dirahasiakan, namun apabila ada alasan yang dapat dibenarkan oleh

Undang-Undang, rahasia bank mengenai keuangan nasabah yang bersangkutan boleh dibuka kepada pejabat yang berwenang.

Hasil penelitian ini mengindikasikan bahwa dengan adanya perlindungan nasabah berupa kerahasiaan data nasabah dapat menjamin terjaga dan keamanannya data nasabah yang ada dan diterima oleh bank. Sehingga apabila terjadi tindak kejahatan *cyber*, pihak bank juga harus ikut bertanggung jawab dalam menanganinya.

4. Pengaruh *Test and Trial Drive* terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta

Hasil dari penelitian tidak mendukung hipotesis keempat (H4), bahwa variabel *Test and Trial Drive* tidak berpengaruh dan tidak signifikan terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta. Hal ini ditunjukkan oleh nilai koefisien regresi sebesar 0,036. Koefisien regresi X4 sebesar 0,036 menyatakan bahwa setiap kenaikan *Test and Trial Drive* sebesar 1 satuan tidak akan menaikkan *Cyber Crime* sebesar 0,036 satuan. Hal ini berarti model tersebut adalah tidak berpengaruh. Berdasarkan hasil analisis data diperoleh nilai t_{hitung} sebesar 0,187 yang nilainya di bawah t_{tabel} sebesar 1,998. Hasil ini menunjukkan bahwa t_{hitung} lebih kecil dari t_{tabel} , hal ini berarti tidak terdapat pengaruh *Test and Trial Drive* terhadap *Cyber Crime* di DIY. Selain itu nilai probabilitas signifikansi *Test and Trial Drive* sebesar 0,852 yang lebih besar dari 0,05, maka dapat dinyatakan bahwa *Test and Trial Drive* tidak berpengaruh signifikan terhadap *Cyber Crime* di DIY sehingga hipotesis 4 tidak didukung tingkat kepercayaan 95%.

Hasil dalam penelitian ini menyatakan bahwa tidak ada hubungan antara *Test and Trial Drive* dengan *Cyber Crime*. Hal ini dapat didukung melalui teori Roche (2014) bahwa *test and trial drive* ini merupakan salah satu bentuk dari kualitas layanan yang menjadi elemen penting dari kepuasan nasabah. Di dalam aspek *test and trial drive* ini lebih mengedepankan tentang respon yang baik melalui penyediaan fitur *website bank*, respon cepat ketika mengakses *internet banking*, bank melakukan sosialisasi dan edukasi nasabah dalam menggunakan *internet banking* dan diikuti dengan informasi yang jelas pada *website bank* sebagai respon yang baik juga nasabah bisa melakukan *chat online* dengan staf bank yang dapat dihubungi langsung untuk berkomunikasi mengenai kendala dalam menggunakan *internet banking*, *website bank* dengan tampilan yang bagus, serta lebih komunikatif agar dapat dipahami.

Dalam penelitian ini mengindikasi bahwa *test and trial drive* ini lebih mengutamakan pada bagaimana pihak bank memberikan layanan yang baik dan responsif melalui fitur, aplikasi dan *website internet banking* yang dapat diakses kapan saja dan dimana saja. Sehingga aspek *test and trial drive* ini cenderung mengutamakan kepada kepuasan nasabah pengguna produk *internet banking*.

5. Pengaruh *Customer Support Service* terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta

Hasil dari penelitian mendukung hipotesis kelima (H5), bahwa variabel *Customer Support Service* berpengaruh positif dan signifikan

terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta. Hal ini ditunjukkan oleh nilai koefisien regresi sebesar 0,528. Koefisien regresi X5 sebesar 0,528 menyatakan bahwa setiap kenaikan *Customer Support Service* sebesar 1 satuan akan menaikkan *Cyber Crime* sebesar 0,528 satuan. Hal ini berarti model tersebut adalah positif. Berdasarkan hasil analisis data diperoleh nilai t_{hitung} sebesar 2,514 yang nilainya di atas t_{tabel} sebesar 1,998. Hasil ini menunjukkan bahwa t_{hitung} lebih besar dari t_{tabel} , hal ini berarti terdapat pengaruh positif *Customer Support Service* terhadap *Cyber Crime* di DIY. Selain itu nilai probabilitas signifikansi *Customer Support Service* sebesar 0,014 yang lebih kecil dari 0,05, maka dapat dinyatakan bahwa *Customer Support Service* berpengaruh signifikan terhadap *Cyber Crime* di DIY sehingga hipotesis 1 didukung tingkat kepercayaan 95%.

Hasil penelitian ini menjelaskan bahwa semakin baik pelayanan yang diberikan pihak bank akan membuat nasabah akan semakin loyal dalam menggunakan produk *internet banking*. Hal ini sesuai dengan teori dari Kasmir (2003) bahwa *customer service* ini memegang peranan sangat penting dalam perusahaan maupun bank. Oleh karena itu tugas *customer service* merupakan tulang punggung kegiatan operasional dunia perbankan. Peranan *customer service* adalah mempertahankan nasabah lama agar tetap setia menjadi nasabah melalui pembinaan hubungan yang lebih akrab dengan nasabah, sehingga nasabah akan tetap setia menjadi pengguna produk *internet banking* meskipun banyak kejadian seperti kejahatan *cyber* yang terjadi di dunia perbankan. Semakin baik pelayanan yang diberikan

oleh pihak bank seperti *reliability*, *responsiveness*, *assurance*, dan *emphaty*, menurut Lupiyoadi (2001) melalui *Customer Support Service* ini tentunya akan meminimalisir terjadinya *cyber crime*. Sebab, dengan kualitas pelayanan yang baik, nasabah akan merasa bahwa transaksi-transaksi yang dilakukannya selama ini aman.

6. Pengaruh Penggunaan *Internet Banking* dan Perlindungan Nasabah (*Client Charter*, Kerahasiaan Data Nasabah, *Test and Trial Drive*, dan *Customer Support Service*) Secara Bersama-sama terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta

Hasil Penelitian ini mendukung hipotesis keenam (H6) bahwa variabel Penggunaan *Internet Banking*, *Client Charter*, Kerahasiaan Data Nasabah, *Test and Trial Drive*, dan *Customer Support Service* secara bersama-sama berpengaruh positif dan signifikan terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta. Hal ini ditunjukkan oleh nilai koefisien regresi sebesar 0,513. Berdasarkan hasil uji diperoleh nilai F_{hitung} sebesar 4,714 jika dibandingkan dengan nilai F_{tabel} sebesar 2,37 pada taraf signifikansi 5% maka nilai $F_{hitung} > F_{tabel}$ sehingga Penggunaan *Internet Banking* (X1), *Client Charter* (X2), Kerahasiaan Data Nasabah (X3), *Test and Trial Drive* (X4), dan *Customer Support Service* (X5) secara bersama-sama berpengaruh signifikan terhadap *Cyber Crime* (Y). Berdasarkan hasil analisis data didapat *adjusted R²* sebesar 0,263. Nilai tersebut berarti 26,3% variabel dependen *Cyber Crime* dapat diterangkan oleh variabel-variabel

independennya, sedangkan sisanya sebesar 73,7% dijelaskan oleh variabel yang lain yang tidak dianalisis dalam penelitian ini.

Hasil penelitian ini mendukung jurnal yang dikeluarkan oleh Direktorat Penelitian dan Pengaturan Perbankan Bank Indonesia yaitu pengamanan data transaksi maupun data nasabah merupakan suatu hal yang sangat penting dalam *internet banking*. Keselamatan dan keamanan data transaksi dari segala gangguan sadapan maupun pencurian dari pihak manapun harus dilindungi. Begitu halnya dengan data dan informasi nasabah bank pemakai jasa *internet banking* juga harus mendapatkan perlindungan. Perlindungan data transaksi dan nasabah tersebut akan lebih kuat dan mempunyai kekuatan hukum yang pasti apabila diatur dalam bentuk undang-undang atau peraturan.

Keamanan dan keselamatan data nasabah ini dijabarkan melalui bentuk perlindungan nasabah seperti yang sudah dijelaskan yaitu *client charter*, kerahasiaan data nasabah, *test and trial drive*, dan *customer support service*. Sehingga dengan adanya perlindungan nasabah pengguna fasilitas *internet banking* ini diharapkan mampu mencegah terjadinya *cyber crime* yang marak terjadi di era digital seperti saat sekarang ini.

C. Keterbatasan Penelitian

Penelitian ini telah diusahakan dan dilakukan sesuai dengan prosedur ilmiah, akan tetapi masih memiliki keterbatasan antara lain:

1. Dalam pengumpulan data, penelitian ini menggunakan kuesioner. Oleh karena itu, data yang terkumpul hanya menggambarkan persepsi para

responden pada saat menerjemahkan pernyataan-pernyataan yang ada sesuai persepsi para responden. Karena itu, kemungkinan terjadinya bias sangat memungkinkan, hal ini disebabkan perbedaan persepsi antara peneliti dan para responden terhadap pernyataan-pernyataan yang diajukan dan diterima.

2. Temuan hasil penelitian membuktikan bahwa selain Penggunaan *Internet Banking* dan Perlindungan Nasabah terdapat faktor-faktor lain yang mempengaruhi *Cyber Crime* di Daerah Istimewa Yogyakarta dengan bukti bahwa Penggunaan *Internet Banking* dan Perlindungan Nasabah hanya memberikan sumbangan sebesar 26,3% terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta, sedangkan 73,7% dijelaskan faktor lain yang tidak diteliti dalam penenlitian ini.

BAB V

SIMPULAN DAN SARAN

A. Simpulan

1. Terdapat pengaruh positif dan signifikan Penggunaan *Internet Banking* terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta. Hal tersebut dapat ditunjukkan dengan nilai koefisien regresi sebesar 0,281. Pada taraf signifikansi 5%, dapat diketahui t_{hitung} sebesar 2,124 dengan nilai signifikansi 0,037 karena koefisien regresi mempunyai nilai positif dan nilai signifikansi (p) < 0,05 maka dapat disimpulkan terdapat pengaruh positif dan signifikan Penggunaan *Internet Banking* terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta.
2. Pengaruh Perlindungan Nasabah terhadap *Cyber Crime* masing-masing dapat dijelaskan sebagai berikut:
 - a. Terdapat pengaruh negatif dan signifikan *Client Charter* terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta. Hal tersebut dapat ditunjukkan dengan nilai koefisien regresi sebesar -0,591. Pada taraf signifikansi 5%, dapat diketahui t_{hitung} sebesar -2,341 dengan nilai signifikansi 0,022 karena koefisien regresi mempunyai nilai negatif dan nilai signifikansi (p) < 0,05 maka dapat disimpulkan terdapat pengaruh negatif dan signifikan *Client Charter* terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta.
 - b. Terdapat pengaruh positif dan signifikan Kerahasiaan Data Nasabah terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta. Hal tersebut

dapat ditunjukkan dengan nilai koefisien regresi sebesar 0,630. Pada taraf signifikansi 5%, dapat diketahui t_{hitung} sebesar 2,518 dengan nilai signifikansi 0,014 karena koefisien regresi mempunyai nilai positif dan nilai signifikansi (p) < 0,05 maka dapat disimpulkan terdapat pengaruh positif dan signifikan Kerahasiaan Data Nasabah terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta.

- c. Tidak terdapat pengaruh dan tidak signifikan *Test and Trial Drive* terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta. Hal tersebut dapat ditunjukkan dengan nilai koefisien regresi sebesar 0,036. Pada taraf signifikansi 5%, dapat diketahui t_{hitung} sebesar 0,187 dengan nilai signifikansi 0,852 karena koefisien regresi mempunyai nilai positif dan nilai signifikansi (p) > 0,05 maka dapat disimpulkan tidak terdapat pengaruh dan tidak signifikan *Test and Trial Drive* terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta.
- d. Terdapat pengaruh positif dan signifikan *Customer Support Service* terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta. Hal tersebut dapat ditunjukkan dengan nilai koefisien regresi sebesar 0,528. Pada taraf signifikansi 5%, dapat diketahui t_{hitung} sebesar 2,514 dengan nilai signifikansi 0,014 karena koefisien regresi mempunyai nilai positif dan nilai signifikansi (p) < 0,05 maka dapat disimpulkan terdapat pengaruh positif dan signifikan *Customer Support Service* terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta.

3. Terdapat pengaruh Penggunaan *Internet Banking*, dan Perlindungan Nasabah Pengguna Fasilitas *Internet Banking* (*Client Charter*, Kerahasiaan Data Nasabah, *Test and Trial Drive*, dan *Customer Support Service*) terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta. Hal tersebut dapat ditunjukkan dengan nilai F_{hitung} sebesar 4,714 dengan nilai signifikansi 0,001. Karena nilai signifikansi $F < 0,05$ maka terdapat pengaruh Penggunaan *Internet Banking*, *Client Charter*, Kerahasiaan Data Nasabah, *Test and Trial Drive*, dan *Customer Support Service* secara bersama-sama terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta. Nilai koefisien determinasi (R^2) sebesar 0,263 atau 26,3%. Nilai koefisien determinasi tersebut menunjukkan 26,3% terjadinya *Cyber Crime* dapat dijelaskan oleh variabel Penggunaan *Internet Banking*, *Client Charter*, Kerahasiaan Data Nasabah, *Test and Trial Drive*, dan *Customer Support Service*, sedangkan sisanya sebesar 73,3% dijelaskan oleh variabel lain yang tidak diteliti dalam penelitian ini. Sumbangan efektif masing-masing variabel yaitu 8,30% untuk variabel Penggunaan *Internet Banking*, 18,50% untuk variabel *Client Charter*, 19,07% untuk Kerahasiaan Data Nasabah, 1,08% untuk variabel *Test and Trial Drive*, dan 16,34% untuk variabel *Customer Support Service*.

B. Implikasi

1. Penggunaan *Internet Banking* berkaitan dengan terjadinya *Cyber Crime* mengingat *trend* menggunakan transaksi *banking* yang meningkat sehingga dapat menimbulkan kejahatan *cyber crime*. Hasil penelitian menunjukkan bahwa Penggunaan *Internet Banking* berpengaruh terhadap terjadinya *Cyber*

Crime di DIY. Hal ini mengandung implikasi agar kedepannya pihak bank mampu meningkatkan sistem keamanan khususnya bagi produk perbankan yang berbasis *internet*.

2. *Client Charter* merupakan komitmen bank untuk memberikan pelayanan yang andal dan berkualitas. Hasil penelitian ini menunjukkan bahwa *Client Charter* berpengaruh terhadap *Cyber Crime* di DIY. Hal ini mengandung implikasi agar kedepannya pihak bank dapat memberikan pelayanan publik yang lebih tanggap atau responsif, transparan, serta bertanggungjawab penuh terhadap semua keluhan dan kendala yang dihadapi nasabah.
3. Kerahasiaan Data Nasabah merupakan kebijakan bank untuk menjaga dan menghargai *privacy* nasabah atas informasi personal nasabah. Hasil penelitian menunjukkan bahwa Kerahasiaan Data Nasabah berpengaruh terhadap *Cyber Crime* di DIY. Hal ini mengandung implikasi bahwa kerahasiaan mengenai nasabah dan keuangannya tidak boleh dibuka dengan alasan apapun dan oleh siapapun. Pihak bank harus mampu memberi keyakinan dan kepercayaan pada seluruh nasabahnya bahwa transaksi yang dilakukan nasabah aman dan terjaga kerahasiannya.
4. *Test and Trial Drive* merupakan panduan penggunaan untuk nasabah dalam menggunakan fitur dan fungsi pada *website* atau aplikasi *internet banking*. Hasil penelitian menunjukkan bahwa *Test and Trial Drive* tidak berpengaruh terhadap *Cyber Crime* di DIY. Hal ini mengandung implikasi bahwa *test and trial drive* cenderung hanya mengedepankan permasalahan mengenai tampilan aplikasi dan *website* situs saja dan pihak bank hanya

lebih mengutamakan kepuasan nasabah dalam menjalankan situs aplikasi dan *website* serta memberikan panduan penggunaannya.

5. *Customer Support Service* merupakan layanan untuk nasabah yang diberikan bank yang dapat diakses 24 jam. Hasil penelitian menunjukkan bahwa *Customer Support Service* berpengaruh terhadap *Cyber Crime* di DIY. Hal ini mengandung implikasi bahwa semakin baik pelayanan yang diberikan pihak bank maka nasabah akan semakin loyal dalam menggunakan produk *internet banking*, dengan kualitas layanan yang baik inilah yang akan membuat nasabah tetap setia menggunakan internet banking meskipun kejadian *cyber crime* sering terjadi dalam dunia perbankan.

C. Saran

Berdasarkan hasil penelitian dan kesimpulan di atas maka dapat diberikan saran-saran sebagai berikut:

1. Bagi Bank

a. Penelitian ini memberikan informasi bahwa nasabah masih merasakan kekhawatiran apabila memberikan informasi keuangannya saat melakukan transaksi melalui *internet banking*. Dengan adanya infomasi ini diharapkan dapat memberi masukan pada pihak bank untuk lebih meningkatkan keamanan layanan *internet banking* dan lebih intensif dalam melakukan sosialisasi keamanan dalam penggunaan layanan *internet banking*.

b. Selain itu juga diharapkan adanya bentuk perlindungan untuk nasabah yang secara khusus diatur untuk melindungi nasabah dari tindak kejahatan *cyber crime* yang marak terjadi saat ini. Diharapkan bank mampu membuat semacam aplikasi unit untuk melaporkan setiap kejahatan *cyber crime* serta membangun pencegahan atau pertahanan anti *malware* di seluruh *server* bank.

2. Bagi Nasabah

Penelitian ini memberikan informasi bahwa nasabah wajib memperhatikan resiko yang dapat ditimbulkan dari adanya *internet banking* ini tidak hanya melihat dari segi kemudahannya saja. Dengan mengetahui resiko yang dapat terjadi ini nasabah dapat mawas diri dan hati-hati dalam menggunakan *internet banking*.

3. Bagi Penelitian Selanjutnya

Penelitian ini memberikan informasi bahwa Penggunaan *Internet Banking*, *Client Charter*, Kerahasiaan Data Nasabah, *Test and Trial Drive*, dan *Customer Support Service* memberikan sumbangan sebesar 26,3% terhadap *Cyber Crime* di Daerah Istimewa Yogyakarta, sedangkan 73,3% dijelaskan faktor lain yang tidak diteliti dalam penelitian ini. Untuk itu perlu adanya penelitian lebih lanjut tentang faktor-faktor yang dapat mempengaruhi terjadinya *Cyber Crime* di dunia perbankan khususnya. Penelitian selanjutnya juga disarankan untuk lebih memfokuskan variabel penelitiannya tidak hanya lingkup keamanan dan perlindungan nasabah saja, perlindungannya juga bisa dilihat dari segi perlindungan hukum atau

perlindungan dari pemerintah sehingga cakupan penelitiannya bisa lebih luas lagi.

DAFTAR PUSTAKA

- Arifah Amalia, Dista. (2011). “Kasus Cyber Crime di Indonesia”. Jurnal Bisnis dan Ekonomi. Vol.18 No.2. FE UNISSULA. Semarang.
- Arikunto, Suharsimi. (2000). “Manajemen Penelitian”. Jakarta: PT.Rineka Cipta.
- Arya Wijaya, Muchamad. (2016). “Pengungkapan Data Nasabah yang Dilakukan oleh Pers Ditinjau dari Prinsip Kerahasiaan Bank”. Jurnal Hukum. Yogyakarta: Fakultas Hukum, Universitas Atma Jaya.
- Ayu Astrini, Dwi. (2015). “Perlindungan Hukum Terhadap Nasabah Bank Pengguna Internet Banking dari Ancaman Cybercrime”. Lex Privatum. Vol.III/No.1.
- Danuari, Muhamad. (2017). “Trend Cyber Crime dan Teknologi Informasi di Indonesia”. INFOKAM Nomor 2 Th. XIII/September/2017. Semarang: Universitas Dian Nuswantoro.
- Direktorat Penelitian dan Pengaturan Perbankan Bank Indonesia. (2002). “Internet Banking di Indonesia”. Buletin Ekonomi Moneter dan Perbankan.
- Dzurotun Nisa, Dede, dkk. (2013). “Analisis Faktor-faktor yang Mempengaruhi Nasabah Menggunakan Layanan Internet Banking Mandiri”. Jurnal Manajemen. Vol.13 No.1. Manajemen Bisnis Telekomunikasi dan Informatika, Universitas Telkom.
- Emayasilia. (2012). “Teori Pelayanan”. Diakses dari <https://emayasilia.wordpress.com/2012/10/17/teori-pelayanan/>
- Estradiyanto, Niko. (2012). “Perlindungan Bagi Nasabah Bank dalam Penggunaan Fasilitas *Internet Banking* atas Terjadinya *Cyber Crime* di Indonesia”. Skripsi. Universitas Sebelas Maret Surakarta. Diakses dari <https://digilib.uns.ac.id/dokumen/detail/28503/Perlindungan-bagi-Nasabah-Bank-dalam-Penggunaan-Fasilitas-Internet-Banking-Atas-Terjadinya-Cyber-Crime-di-Indonesia-pada-5-Januari-2018>.
- Ghozali, Imam. (2006). “Aplikasi Analisis Multivariate dengan Program SPSS”. (Edisi ke-4). Semarang: Badan Penerbit Universitas Diponegoro.
- Hadi, Sutrisno. (2004). “Analisis Regresi”. Yogyakarta: ANDI.
- Hermawan, Rudi. (2013). “Kesiapan Aparatur Pemerintah dalam Menghadapi *Cyber Crime* di Indonesia”. Faktor Exacta 6(1): 43-50. ISSN: 1979-276x. Fakultas Teknik, Matematika, dan IPA Universitas Indraprasta PGRI. Jakarta

- Maani, Karjuni. (2010). “*Citizen Charter*: Terobosan Baru dalam Penyelenggaraan Layanan Publik”. TINGKAP Vol. VI No. 2.
- Maria, Antonius. (2015). “Tindak Pidana *Credit/Debit Card Fraud* dan Penerapan Sanksi Pidananya dalam Hukum Pidana Indonesia”. Hasanuddin Law Review. Vol. 1 No. 1. Sekolah Tinggi Ilmu Hukum Manokwari.
- Mathilda, Fiorida. (2012). “*Cyber Crime* dalam Sistem Hukum Indonesia (*Cyber Crime In Indonesia Law System*)”. Sigma-Mu. Vol.4 No.2. UP MKU Politeknik Negeri Bandung.
- Muhson, Ali. (2015). “Pedoman Praktikum Aplikasi Komputer Lanjut”. Yogyakarta: Fakultas Ekonomi, UNY.
- Purnama Alamsyah, Doni, Anugrah, Rizki. (2015). “Membangun Kepercayaan Nasabah pada Internet Banking”. Ecodemica. Vol III. No 2. AMIK BSI Bandung, Universitas BSI Bandung.
- Putri Harry, Nidia. (2015). “Perlindungan Hukum Terhadap Nasabah Bank Pengguna Fasilitas Internet Banking Atas Tejadinya *Cyber Crime* (Studi Kasus: *Bussines Banking Center Mandiri Padang*)”. Skripsi. Universitas Bung Hatta Padang. Diakses dari [http://ejurnal.bunghatta.ac.id/index.php?journal=JFH&page=article&op=viewFile&path\[\]&path\[\]](http://ejurnal.bunghatta.ac.id/index.php?journal=JFH&page=article&op=viewFile&path[]&path[]) pada 10 Januari 2018.
- Raditio, Resa. (2014). “Aspek Hukum Transaksi Elektronik; Perikatan, Pembuktian, dan Penyelesaian Sengketa”. Yogyakarta: Graha Ilmu.
- Rehulina, Hatialum. (2012). “Analisis Yuridis Kejahatan *Cyber Crime* dalam Pembobolan Mesin ATM Bank”. Skripsi. Universitas Pembangunan Nasional “Veteran” Jawa Timur. Diakses dari <http://eprints.upnjatim.ac.id/3642/1/file1.pdf> pada 10 Januari 2018.
- Riduwan. (2007). “Skala Pengukuran Variabel-Variabel Penelitian”. Bandung: Alfabeta.
- Ronny. (2017). “Enam Kekuatan Layanan Jasa *Internet Banking*: Tinjauan dari Persepsi Nasabah”. Jurnal Organisasi dan Manajemen Volume 13, Nomor 2. Suarbaya:STIE Perbanas.
- Savitri Anggraeni, Ni Made, Kerti Yasa, Ni Nyoman. (2012). “E-Service Quality Terhadap Kepuasan dan Loyalitas Pelanggan dalam Penggunaan Internet Banking”. Jurnal Keuangan dan Perbankan. Vol.16 No.2. FE Universitas Udayana. Denpasar.
- Sugiyono. (2012). “Statistika untuk Penelitian”. Bandung: Alfabeta.

Suharjo, Bambang. (2013). "Statistika Terapan Disertai Contoh Aplikasi dengan SPSS". Yogyakarta:Graha Ilmu.

Sujarweni, Wiratna,dkk. (2012). "Statistika untuk Penelitian". Yogyakarta:Graha Ilmu.

Sunyoto, Danang. (2011). "Analisis Regresi dan Uji Hipotesis". Yogyakarta: CAPS.

Taswan. (2010). "Manajemen Perbankan". Yogyakarta: UPP STIM YKPN.

Tianotak, Nazarudin. (2011). "Urgensi *Cyberlaw* di Indonesia dalam Rangka Penanganan *Cyber Crime* di Sektor Perbankan". Jurnal Sasi. Volume 17 No.4.

Tua Hasugian, Saut Manatar. (2013). "Kendala Polda DIY dalam Mengungkap Tindak Pidana Penipuan Melalui Internet di Provinsi Daerah Istimewa Yogyakarta". Jurnal Ilmiah. FH Universitas Atma Jaya Yogyakarta.

Wonok, David. (2013). "Perlindungan Hukum Atas Hak-hak Nasabah Sebagai Konsumen Pengguna Jasa Bank terhadap Resiko yang Timbul dalam Penyimpangan Dana". Vol.I/No.2/April-Juni/2013 Edisi Khusus.

<https://teorionline.wordpress.com/tag/sampel-populasi-penelitian-teknik-sampling/> diakses pada 5 Januari 2018.

<https://sharingvision.com/keamanan-dan-kemudahan-survei-jumlah-pengguna-internet-banking-2011-2012/> diakses pada 5 Januari 2018

<https://sharingvision.com/revolusi-transaksi-elektronik/> diakses pada 5 Januari 2018.

<https://proxsisgroup.com/articles/waspadailah-hantaman-serangan-cyber-terhadap-indonesia/> diakses pada 5 Januari 2018

<http://budi.insanmusic.com/indo-internet.html> diakses pada 5 Januari 2018
<https://inet.detik.com/security/d-2592234/pasukan-cyber-indonesia-harus-dipimpin-presiden> diakses pada 5 Januari 2018.

<https://itgid.org/serangan-cyber-crime-di-indonesia/> diakses pada 5 Januari 2018.

<https://inet.detik.com/consumer/d-464687/pengguna-internet-yogyakarta-capai-17> diakses pada 14 Maret 2018

LAMPIRAN

Lampiran 1. Instrumen Penelitian

**PERLINDUNGAN BAGI NASABAH BANK DALAM PENGGUNAAN
FASILITAS INTERNET BANKING ATAS TERJADINYA CYBER CRIME
DI DAERAH ISTIMEWA YOGYAKARTA (DIY)**

Assalamualaikum, wr.wb.

Saya ucapan terima kasih sebelumnya karena Bapak/Ibu/Sdr bersedia berpartisipasi dalam memperlancar penelitian saya. Adapun penelitian ini dilakukan dalam rangka penulisan tugas akhir sebagai salah satu syarat kelulusan pada jurusan Pendidikan Ekonomi Fakultas Ekonomi Universitas Negeri Yogyakarta. Saya menjamin kerahasiaan anda sebagai kode etik penelitian.

Hormat saya,

Yuslia Naili Rahmah

A. Petunjuk Pengisian

Mohon mengisi kuesioner ini dengan cara memberi tanda check list (✓) pada kolom lembar berikut, yaitu dengan memilih alternatif jawaban yang tersedia. Ada lima alternatif jawaban, yaitu:

Sangat Setuju	(SS) = 5
Setuju	(S) = 4
Kurang Setuju	(KS) = 3
Tidak Setuju	(TS) = 2
Sangat Tidak Setuju	(STS) = 1

B. Identitas Responden

1. Nama :
2. Jenis Kelamin : (P/L) *coret yang tidak perlu
3. Umur :

4. Pekerjaan :

5. Rata-rata menggunakan produk Interenet banking dalam 1 bulan

- a. Tidak pernah
- b. 1 – 3 kali
- c. 4 – 6 kali
- d. 7 – 10 kali
- e. > 10 kali

6. Lama menggunakan produk Internet Banking

- a. <1 tahun
- b. 1 – 2 tahun
- c. 3 – 4 tahun
- d. 4 – 5 tahun
- e. > 5 tahun

C. ANGKET TENTANG PERLINDUNGAN DATA NASABAH

PENGGUNA FASILITAS *INTERNET BANKING*

No.	Pernyataan	Alternatif Jawaban				
		1	2	3	4	5
		STS	TS	KS	S	SS
PENGGUNAAN <i>INTERNET BANKING</i>						
1.	Saya bertransaksi melalui <i>internet banking</i> secara intensif atau minimal dalam satu bulan melakukan transaksi.					
2.	Dengan menggunakan <i>internet banking</i> menjadikan pekerjaan saya menjadi lebih mudah.					
3.	Saya menggunakan <i>internet banking</i> untuk					

	mengakses informasi (misal: saldo, informasi tagihan kartu kredit, dll.)				
4.	Saya menggunakan <i>internet banking</i> untuk melakukan pembayaran tagihan (misal: pembayaran telepon, listrik, pajak, kartu kredit, dll)				
5.	Saya menggunakan <i>internet banking</i> untuk melakukan pembelian (misal: tiket pesawat, voucher isi ulang, dll)				
6.	Saya akan selalu menggunakan <i>internet banking</i> untuk melakukan transaksi karena mempunyai <i>fitur</i> yang membantu pekerjaan saya.				
7.	Dengan <i>internet banking</i> menjadikan waktu saya lebih efektif dalam melakukan transaksi.				
8.	Menggunakan <i>internet banking</i> sangat fleksibel karena dapat dilakukan kapan saja dan dimana saja.				
9.	Saya merasakan menggunakan <i>internet banking</i> dapat memberikan peruntungan saya dimasa depan.				
CLIENT CHARTER					
11.	Pengendalian yang diberikan bank cukup baik untuk melindungi data pribadi dan keuangan saya.				
12.	Membuat nasabah merasa aman ketika melakukan transaksi.				
13.	Bukti pada setiap transaksi pada <i>internet banking</i> yang lengkap disertai waktu transaksinya.				
14.	Saya yakin semua data yang diproses lewat <i>internet banking</i> tidak akan disalahgunakan oleh pihak bank.				

15.	Bank memberikan jaminan bahwa uang yang ditransfer/dibayar sampai pada tujuan yang tepat.				
16.	Saya bisa bertransaksi melalui <i>internet banking</i> walaupun tidak ada orang lain di sekitar saya untuk memberitahu saya bagaimana cara menggunakannya.				
17.	Saya menggunakan <i>internet banking</i> pada bank berdasarkan pertimbangan tingkat privatisasi data.				
18.	Interaksi saya dengan <i>internet banking</i> jelas dan mudah dipahami.				
19.	Saya tidak melakukan kesalahan-kesalahan berlanjut ketika mengoperasikan <i>internet banking</i> .				
20.	Cara karyawan dalam melayani nasabah menimbulkan kepercayaan nasabah kepada bank.				

KERAHASIAAN DATA NASABAH

21.	Bank dapat dipercaya.				
22.	Bank memberikan keamanan data transaksi yang dilakukan.				
23.	Bank memberikan keamanan dalam bertransaksi.				
24.	Kerahasiaan data saya terjamin dalam transaksi <i>internet banking</i> .				
25.	Saya tidak khawatir memberikan informasi keuangan bila bertransaksi melalui <i>internet banking</i> .				
26.	Meskipun ada berita negatif mengenai <i>internet banking</i> , saya percaya dan tidak ragu dalam melakukan transaksi perbankan melalui <i>internet banking</i> .				
27.	Saya yakin semua data yang diproses melalui <i>internet banking</i> tidak akan				

	disalahgunakan oleh pihak bank.				
28.	Setiap kali nasabah menghadapi masalah, bank akan memberikan perhatian terhadap penyelesaian masalah tersebut.				
29.	Nasabah mengetahui dengan baik peraturan perlindungan kerahasiaan datanya.				
30.	Nasabah mengganti <i>Personal Identification Numbernya</i> (PIN) secara berkala.				
TEST AND TRIAL DRIVE					
31.	Situs <i>website</i> bank menyediakan informasi yang dibutuhkan secara cepat dan benar.				
32.	Aplikasi internet banking dapat dengan mudah diakses menggunakan smartphone.				
33.	Situs <i>website</i> dan aplikasiinternet banking menyediakan informasi sesuai dengan kebutuhan nasabah.				
34.	Penyediaan informasi dari aplikasi selalu <i>up to date</i> .				
35.	Semua layanan yang dibutuhkan nasabah sudah ada di <i>website</i> dan aplikasi internet banking di <i>handphone</i> .				
36.	Konten pada aplikasi mudah dimengerti nasabah.				
37.	Ada petunjuk penggunaan alur pada tiap transaksi.				
38.	Kecepatan dalam mengakses situs bank.				
39.	Saya merasa sistem aplikasi yang digunakan dalam internet banking tidak rumit.				
40.	Mudah bagi saya untuk mempelajari bagaimana cara menggunakan <i>internet banking</i> .				
CUSTOMER SUPPORT SERVICE					
41.	Kemampuan petugas <i>customer service</i> dalam menjawab pertanyaan cukup				

	meyakinkan saya bahwa masalah dapat diselesaikan.				
42.	Petugas <i>customer service</i> berkomunikasi dengan bahasa yang mudah dimengerti.				
43.	Sistem informasi bank menjamin solusi yang cepat.				
44.	Saya mendapatkan pelayanan yang segera saat membutuhkan.				
45.	Keluhan saya dapat ditangani dengan baik oleh petugas <i>customer service</i> .				
46.	Setiap saya menyampaikan keluhan atau pertanyaan petugas <i>customer service</i> mendengarkan dengan penuh perhatian.				
47.	Kecepatan pemrosesan keluhan nasabah.				
48.	<i>Customer service online</i> bank tersedia 24 jam.				
49.	Nomor telepon pelayanan ataupun <i>website</i> mudah diakses.				
50.	Sungguh-sungguh mengutamakan kepentingan nasabah.				

D. ANGKET TENTANG TERJADINYA CYBER CRIME

No.	Pernyataan	Alternatif Jawaban				
		1	2	3	4	5
		STS	TS	KS	S	SS
1.	Saya sudah pernah mengalami kejahatan <i>cyber</i> dalam dunia perbankan khususnya.					
2.	Saya pernah mengalami <i>cyber crime</i> berupa <i>craaking, hacking</i> , ataupun yang lain.					
3.	Bank memberikan ganti rugi atas kejahatan yang menimpa saya.					

4.	Saya merasa takut menggunakan fasilitas <i>internet banking</i> karena sudah menjadi korban kejahatan <i>cyber</i> .					
5.	Bank menindaklanjuti dengan cepat kejahatan <i>cyber</i> yang saya alami.					
6.	Bank memberikan perlindungan yang tepat bagi nasabahnya.					
7.	Bank segera melakukan evaluasi ketika setelah terjadi kejahatan <i>cyber</i> yang melibatkan nasabahnya.					
8.	Bank selalu memberikan sosialisasi tentang kejahatan <i>cyber</i> yang bisa terjadi kapanpun kepada nasabah.					
9.	Saya akan tetap menggunakan <i>internet banking</i> walaupun sudah menjadi korban kejahatan <i>cyber</i> .					
10.	Nasabah mengetahui undang-undang atau peraturan yang mengatur secara khusus tentang <i>cyber crime</i> .					

Resp	Jawaban Pertanyaan Variabel X1 (Penggunaan <i>Internet Banking</i>)										Total
	1	2	3	4	5	6	7	8	9	10	
1	5	4	5	4	3	5	4	5	4	4	43
2	4	4	4	5	4	5	5	4	4	4	43
3	4	5	3	3	4	5	4	3	3	4	38
4	4	5	4	4	4	4	4	4	4	4	41
5	2	3	2	3	3	3	3	3	3	3	28
6	2	4	2	3	2	2	2	3	3	3	26
7	4	4	4	4	4	4	3	3	3	3	36
8	4	4	4	5	3	4	3	4	4	4	39
9	4	4	3	4	4	3	4	4	4	5	39
10	2	4	4	4	2	3	3	3	4	4	33
11	1	2	1	2	2	2	1	2	3	2	18
12	5	4	4	4	4	4	4	5	4	5	43
13	1	1	1	1	1	1	1	1	1	2	11
14	4	3	3	4	3	3	3	3	3	4	33

15	4	4	4	4	3	4	3	4	3	3	36
16	4	4	5	4	3	3	4	4	4	4	39
17	4	4	4	4	4	5	5	5	5	5	45
18	4	4	3	3	3	3	4	4	3	3	34
19	2	4	4	4	4	4	3	3	3	3	34
20	3	3	3	3	3	3	4	4	4	4	34
21	3	3	3	4	4	4	2	4	4	3	34
22	4	4	4	4	3	4	4	5	5	3	40
23	3	3	4	4	3	3	3	4	4	4	35
24	2	4	2	4	2	4	3	3	3	3	30
25	2	4	4	4	3	4	4	3	5	4	37
26	4	5	4	5	3	3	4	4	4	3	39
27	1	3	4	4	1	1	1	3	3	3	24
28	3	3	3	4	4	4	4	4	5	3	37
29	3	3	3	3	4	4	4	4	4	4	36
30	2	3	3	5	4	5	4	4	4	5	39

31	2	3	3	3	3	3	3	3	3	3	3	29
32	2	4	2	4	3	3	4	5	5	4	36	
33	3	3	3	3	4	4	4	4	4	4	36	
34	4	4	2	4	2	2	2	4	4	4	32	
35	4	4	4	4	4	4	4	5	4	4	41	
36	5	5	5	4	4	5	4	5	5	5	47	
37	3	5	4	4	3	3	3	4	5	4	38	
38	4	5	4	5	4	4	4	5	4	3	42	
39	4	4	4	4	4	4	4	4	4	4	40	
40	4	5	5	5	5	5	5	5	5	5	49	
41	5	5	5	5	5	5	5	5	5	5	50	
42	5	5	5	5	5	4	4	5	4	4	46	
43	4	4	4	4	4	4	4	4	4	4	40	
44	4	5	4	4	2	4	5	5	5	4	42	
45	4	5	4	5	4	5	4	5	4	3	43	
46	3	4	4	4	4	2	2	4	4	4	35	

47	4	5	4	5	4	4	4	4	3	4	41
48	4	4	4	4	4	2	4	4	4	4	38
49	1	4	2	2	1	1	3	4	4	4	26
50	1	4	4	4	1	4	4	4	5	5	36
51	4	5	4	4	4	4	4	5	4	3	41
52	2	2	4	4	4	3	3	2	4	4	32
53	4	5	5	5	2	5	5	5	5	5	46
54	3	4	4	4	4	3	3	4	4	4	37
55	3	4	4	4	3	3	3	4	4	4	36
56	4	5	4	4	4	4	4	5	5	4	43
57	4	4	4	4	4	5	5	5	5	4	44
58	3	4	5	5	4	3	3	4	4	4	39
59	5	5	5	4	2	3	4	5	4	3	40
60	2	5	3	4	4	4	4	4	4	4	38
61	4	4	4	4	4	4	4	4	4	4	40
62	2	4	4	2	2	2	4	4	4	3	31

63	4	5	4	5	2	4	5	5	5	4	43
64	4	5	5	4	3	4	4	4	4	4	41
65	4	5	4	4	4	4	5	5	5	4	44
66	5	5	5	5	5	5	5	5	5	5	50
67	5	5	5	4	2	2	4	4	5	4	40
68	4	4	5	4	3	5	4	4	5	4	42
69	4	4	4	4	4	4	4	4	4	4	40
70	4	4	3	4	4	4	4	4	4	4	39
71	4	5	4	4	4	4	5	5	5	5	45
72	4	4	4	4	3	3	4	4	4	4	38

Resp	Jawaban Pertanyaan Variabel X2 (<i>Client Charter</i>)										Total
	1	2	3	4	5	6	7	8	9	10	
1	3	3	4	3	4	5	4	4	4	4	38
2	5	5	5	4	5	5	5	5	5	5	49
3	4	4	4	3	3	3	4	4	4	4	37

4	5	5	5	5	5	5	5	5	4	5	49
5	4	4	4	4	4	3	4	4	4	4	39
6	4	3	4	3	4	2	2	4	3	4	33
7	4	4	5	4	4	5	4	4	4	4	42
8	5	5	5	5	5	5	4	5	4	4	47
9	4	4	4	4	4	3	4	4	4	5	40
10	4	4	4	4	4	2	4	4	4	4	38
11	4	3	4	3	4	3	3	3	3	3	33
12	4	4	5	4	5	5	5	5	5	5	47
13	3	3	4	4	4	4	4	1	1	4	32
14	4	3	4	4	4	5	4	4	4	4	40
15	4	3	4	1	3	4	3	4	4	3	33
16	5	5	5	5	5	5	5	5	4	4	48
17	4	4	4	4	4	5	4	4	4	4	41
18	4	4	4	4	4	4	3	4	4	4	39
19	4	4	4	4	4	4	4	5	5	4	42

20	3	4	5	4	4	4	4	4	4	4	40
21	3	3	4	4	4	4	4	4	4	4	38
22	3	4	5	4	5	5	3	4	4	4	41
23	4	4	4	3	4	3	4	4	3	4	37
24	5	5	5	4	4	4	4	4	4	4	43
25	4	4	4	4	4	4	4	4	4	4	40
26	4	3	4	4	4	4	3	4	4	5	39
27	4	4	4	3	3	4	4	4	4	4	38
28	4	4	4	4	4	4	4	4	4	4	40
29	4	3	4	4	4	4	3	3	3	4	36
30	5	5	4	4	4	5	3	5	2	4	41
31	3	3	4	3	3	3	3	4	4	4	34
32	4	4	4	4	4	4	3	3	3	3	36
33	4	4	4	3	3	3	3	4	4	4	36
34	2	3	3	4	4	4	4	4	4	4	36
35	4	3	4	3	3	4	4	4	4	4	37

36	3	4	4	3	4	3	5	4	4	4	38
37	4	4	3	3	3	4	3	4	4	4	36
38	4	4	3	4	4	4	3	4	4	4	38
39	4	4	4	4	4	4	4	4	4	4	40
40	5	4	4	4	4	4	5	5	5	5	45
41	5	5	5	3	5	4	4	4	4	4	43
42	4	4	4	3	4	5	4	4	4	4	40
43	3	4	4	4	4	4	4	4	4	3	38
44	5	4	5	5	5	5	5	5	5	4	48
45	4	4	5	3	5	4	5	4	2	4	40
46	4	4	4	4	4	4	4	4	4	4	40
47	4	4	4	4	4	4	4	4	3	4	39
48	4	4	4	4	4	4	4	4	4	4	40
49	3	3	3	3	3	3	3	3	3	4	31
50	4	5	5	5	5	5	5	5	5	5	49
51	4	4	4	4	4	4	5	4	4	4	41

52	4	5	5	3	4	4	5	4	4	5	43
53	5	5	5	1	5	5	5	5	5	2	43
54	4	4	4	4	4	3	4	3	4	4	38
55	4	4	4	4	4	4	4	4	4	4	40
56	4	4	4	4	4	4	4	4	4	4	40
57	3	3	4	3	4	4	4	4	4	4	37
58	4	4	4	4	4	4	4	4	4	4	40
59	4	4	5	4	5	5	4	5	3	4	43
60	5	5	5	5	5	5	5	5	5	5	50
61	4	4	4	5	5	4	4	4	4	4	42
62	3	4	4	4	4	4	3	4	4	4	38
63	5	5	5	5	5	5	4	5	5	5	49
64	4	4	4	4	4	3	4	4	4	4	39
65	4	4	4	4	4	4	4	4	4	4	40
66	4	4	4	2	4	4	4	4	3	4	37
67	4	4	4	5	4	3	3	4	3	4	38

68	4	4	4	4	4	4	4	4	4	4	4	40
69	4	4	4	4	4	3	4	4	4	4	4	39
70	4	5	4	4	4	5	4	4	4	4	4	42
71	4	4	4	4	4	4	4	4	5	4	4	41
72	4	4	4	4	4	4	4	4	4	4	4	40

Resp	Jawaban Pertanyaan Variabel X3 (Kerahasiaan Data Nasabah)										Total
	1	2	3	4	5	6	7	8	9	10	
1	3	3	3	3	3	4	4	5	4	3	35
2	3	3	3	4	5	5	5	5	4	4	41
3	4	4	4	4	4	4	3	3	3	3	36
4	5	5	4	4	3	3	4	5	4	3	40
5	4	4	3	3	3	3	4	4	4	4	36
6	4	4	4	3	3	3	3	4	4	4	36
7	4	4	4	4	4	3	4	4	3	4	38
8	3	4	4	4	2	4	3	5	4	4	37

9	4	4	4	4	2	4	4	4	4	4	4	38
10	4	4	4	4	2	2	4	4	4	4	4	36
11	4	4	4	4	4	3	3	3	3	3	3	35
12	4	4	4	4	3	3	4	4	4	4	4	38
13	4	3	3	4	4	4	4	4	4	4	4	38
14	4	4	4	4	3	3	4	4	3	4	4	37
15	3	4	3	2	4	4	3	4	3	2	2	32
16	4	4	4	4	4	4	4	4	4	4	4	40
17	4	4	4	4	4	3	4	4	3	3	3	37
18	4	4	4	4	4	4	4	4	4	3	3	39
19	4	4	4	4	4	4	5	4	5	4	4	42
20	4	5	5	3	1	2	3	5	4	4	4	36
21	4	4	4	3	3	3	3	4	4	4	4	36
22	4	4	4	4	3	3	4	4	5	4	4	39
23	4	4	4	4	3	3	3	3	3	4	4	35
24	4	4	4	4	2	2	3	4	4	4	4	35

25	5	4	4	4	2	3	4	3	4	4	37
26	4	4	4	3	2	2	3	4	3	3	32
27	4	4	4	3	3	1	3	3	3	3	31
28	4	4	4	4	4	3	4	4	4	4	39
29	4	4	4	4	3	3	4	4	4	3	37
30	5	4	5	4	4	4	3	4	4	4	41
31	4	3	3	3	4	3	4	4	4	4	36
32	4	3	4	4	4	4	3	4	4	4	38
33	4	4	4	4	4	4	4	4	4	4	40
34	4	4	4	4	4	4	3	4	4	4	39
35	5	5	4	4	4	4	2	4	4	4	40
36	4	4	4	4	4	4	3	4	4	4	39
37	4	4	3	4	5	4	5	4	4	4	41
38	4	3	4	4	4	3	4	4	4	5	39
39	4	4	4	4	4	4	3	4	4	4	39
40	5	5	5	5	5	5	5	5	5	5	50

41	5	4	5	4	4	5	4	5	5	5	5	46
42	4	4	4	4	4	3	4	4	4	4	4	39
43	4	3	3	4	3	4	4	4	4	4	4	37
44	5	5	5	5	5	5	4	5	5	5	5	49
45	5	4	4	3	4	4	3	4	5	4	4	40
46	4	4	4	4	4	4	3	4	4	4	4	39
47	4	4	4	4	4	4	3	4	4	4	4	39
48	4	4	4	4	4	4	4	4	4	4	4	40
49	4	3	3	3	3	3	3	4	4	4	4	34
50	5	5	5	5	5	5	5	5	5	5	5	50
51	4	3	4	4	4	4	5	4	4	4	4	40
52	4	1	1	2	5	4	5	4	5	5	5	36
53	1	1	5	1	5	5	5	1	1	5	30	
54	4	4	4	4	4	4	4	4	4	4	4	40
55	4	4	4	4	4	4	3	4	4	4	4	39
56	4	4	4	4	4	4	3	4	4	4	4	39

57	5	3	4	4	4	4	5	4	4	4	41
58	4	3	4	4	4	4	4	4	4	4	39
59	4	2	4	3	4	4	3	5	4	4	37
60	5	5	5	5	5	5	3	5	5	5	48
61	5	4	5	5	5	4	4	5	5	5	47
62	4	4	2	4	4	3	2	4	4	4	35
63	5	5	4	5	5	5	5	5	5	5	49
64	4	4	4	4	4	4	3	4	4	4	39
65	4	4	4	4	4	4	4	4	4	4	40
66	4	3	2	3	2	2	2	4	4	4	30
67	4	4	3	4	4	4	4	5	4	4	40
68	4	4	4	4	4	4	4	4	4	4	40
69	4	4	4	4	4	4	4	4	4	4	40
70	4	4	4	4	4	4	4	4	4	4	40
71	4	2	3	4	4	4	4	4	4	4	37
72	4	4	4	4	4	4	4	4	4	4	40

Resp	Jawaban Pertanyaan Variabel X4 (<i>Test and Trial Drive</i>)										Total
	1	2	3	4	5	6	7	8	9	10	
1	4	4	4	4	3	3	3	3	4	4	36
2	5	5	4	4	3	3	5	4	4	5	42
3	3	3	4	3	3	4	3	3	3	4	33
4	3	3	3	4	4	4	3	4	4	4	36
5	4	3	3	4	5	4	3	3	4	4	37
6	4	4	4	4	4	3	4	3	4	4	38
7	4	5	4	4	4	4	4	4	4	4	41
8	4	4	4	3	3	4	4	4	4	5	39
9	4	5	5	4	4	4	3	5	5	5	44
10	4	4	3	3	3	5	4	3	3	4	36
11	3	3	3	3	3	3	3	3	3	3	30
12	3	3	3	3	3	3	3	3	2	2	28
13	4	4	4	3	4	3	4	3	4	4	37

14	4	4	5	5	4	4	5	5	5	4	45
15	3	4	4	3	3	3	4	3	3	3	33
16	3	3	3	3	4	4	4	4	4	4	36
17	4	4	4	4	3	4	4	3	3	3	36
18	3	3	3	3	3	3	3	3	3	4	31
19	4	4	3	3	5	5	4	4	3	3	38
20	4	4	4	3	3	3	4	4	3	4	36
21	5	5	5	4	4	4	4	5	5	4	45
22	4	4	4	3	3	4	4	3	4	4	37
23	3	4	3	3	3	3	3	4	3	3	32
24	4	4	4	4	4	4	4	3	5	5	41
25	4	4	3	3	4	4	5	5	4	3	39
26	5	5	4	4	4	5	3	4	4	4	42
27	3	4	5	5	5	3	3	3	4	4	39
28	4	4	4	4	4	5	5	5	5	5	45
29	5	5	5	4	4	4	4	3	4	4	42

30	4	5	4	5	4	5	5	4	5	4	45
31	3	3	4	3	3	3	4	3	4	4	34
32	4	5	4	4	3	3	3	4	4	4	38
33	4	4	4	4	4	4	3	3	3	3	36
34	3	4	4	3	3	3	3	3	4	4	34
35	4	4	5	5	5	4	4	3	3	4	41
36	3	3	3	4	4	5	5	4	3	4	38
37	4	4	4	5	5	5	4	3	4	4	42
38	4	4	5	3	5	4	3	3	4	3	38
39	4	4	3	3	4	4	4	3	3	4	36
40	5	5	5	5	5	5	5	5	5	5	50
41	4	5	4	5	5	5	5	4	4	5	46
42	3	5	4	3	3	4	4	4	5	4	39
43	3	3	3	3	4	4	3	3	3	3	32
44	4	4	4	5	5	4	5	5	5	4	45
45	4	5	3	4	5	4	4	4	4	2	39

46	4	5	4	4	3	4	4	4	4	4	3	39
47	4	3	4	4	4	4	4	3	4	4	4	38
48	5	5	4	5	4	4	5	5	4	4	4	45
49	3	4	3	3	3	3	3	3	3	4	32	
50	5	5	5	5	5	3	5	4	4	5	46	
51	4	5	4	3	4	3	3	3	3	4	36	
52	4	3	3	3	3	4	3	2	3	3	31	
53	4	4	3	3	5	5	5	5	5	2	41	
54	4	3	3	3	3	3	3	3	3	2	30	
55	4	4	4	4	3	3	4	3	4	3	36	
56	4	4	4	3	4	3	3	4	3	4	36	
57	3	4	4	4	4	4	4	5	5	4	41	
58	3	3	3	3	3	3	3	3	3	3	30	
59	4	4	4	4	5	5	4	5	5	5	45	
60	5	5	5	5	5	5	5	5	5	5	50	
61	4	4	4	4	4	5	5	5	5	5	45	

62	4	4	4	4	4	4	4	4	4	4	3	39
63	5	5	5	5	4	5	5	5	4	5	5	48
64	4	4	4	5	5	4	4	5	5	5	5	45
65	4	5	4	4	4	4	4	4	4	4	4	41
66	4	4	3	2	2	2	2	3	3	4	4	29
67	3	2	3	3	4	4	3	4	3	3	3	32
68	4	5	5	4	3	4	4	4	3	3	3	39
69	3	3	4	4	3	4	4	3	4	3	3	35
70	4	4	4	4	4	4	3	3	3	3	3	36
71	4	4	4	3	3	4	3	4	5	4	4	38
72	4	4	3	4	4	4	4	3	3	4	4	37

Resp	Jawaban Pertanyaan Variabel X5 (<i>Customer Support Service</i>)										Total
	1	2	3	4	5	6	7	8	9	10	
1	4	3	3	3	3	4	4	4	4	4	36
2	5	5	5	5	5	4	4	4	5	4	46

3	4	4	4	4	4	4	3	4	4	4	39
4	5	5	5	5	5	5	5	4	4	4	47
5	4	4	4	4	4	4	4	4	3	4	39
6	4	4	4	4	4	4	3	3	3	4	37
7	5	5	4	4	5	5	4	3	3	4	42
8	3	4	4	3	4	4	4	3	4	4	37
9	4	4	4	4	4	4	4	3	4	4	39
10	4	5	5	5	5	4	4	5	4	4	45
11	3	3	3	3	3	3	3	3	4	3	31
12	4	4	5	4	4	4	4	2	1	1	33
13	4	4	4	4	4	4	3	4	3	4	38
14	4	4	4	4	4	4	3	3	4	4	38
15	5	4	5	5	5	5	5	5	5	5	49
16	4	4	4	4	4	4	4	4	4	4	40
17	4	4	4	4	4	4	4	4	4	4	40
18	4	4	4	2	4	4	2	3	3	3	33

19	4	3	4	4	4	4	4	2	3	4	36
20	5	5	5	4	4	4	3	3	4	4	41
21	4	4	4	4	4	4	4	3	4	4	39
22	4	4	4	4	4	4	3	4	4	4	39
23	4	4	4	4	3	4	4	4	4	4	39
24	4	4	4	4	4	4	4	4	4	5	41
25	4	3	4	5	5	5	5	5	5	5	46
26	3	4	3	4	4	4	3	4	3	4	36
27	3	4	3	3	3	3	3	3	4	3	32
28	4	4	3	4	4	4	3	4	4	4	38
29	4	4	4	4	4	4	4	3	4	4	39
30	5	5	5	5	5	5	4	5	3	3	45
31	4	4	4	4	4	4	3	3	3	4	37
32	4	4	4	4	4	4	4	3	4	4	39
33	4	4	4	4	4	4	4	4	4	4	40
34	4	4	4	4	4	4	3	4	4	4	39

35	4	5	4	4	5	4	4	5	4	5	44
36	4	4	4	4	4	4	4	4	4	4	40
37	4	4	4	4	4	4	4	4	4	5	41
38	4	4	4	4	4	4	4	4	4	4	40
39	4	4	4	4	4	4	4	4	4	4	40
40	3	3	5	5	5	5	2	4	3	5	40
41	4	4	4	4	4	4	4	3	4	4	39
42	4	4	4	4	4	4	3	2	4	4	37
43	3	3	3	3	3	4	3	3	3	3	31
44	4	4	4	4	4	4	4	4	4	4	40
45	4	4	3	2	3	4	4	3	4	4	35
46	4	4	4	4	4	5	4	5	5	4	43
47	4	4	4	4	4	4	4	3	3	4	38
48	4	4	4	4	4	4	4	4	4	4	40
49	3	4	3	2	4	4	3	4	3	3	33
50	4	4	4	4	4	4	4	4	4	4	40

51	4	4	4	4	4	4	4	4	4	4	4	40
52	4	5	4	4	4	4	5	4	4	5	43	
53	5	5	5	5	5	5	5	5	5	5	50	
54	3	3	3	3	4	3	3	4	4	4	34	
55	4	4	4	4	4	4	4	4	4	4	40	
56	4	4	4	4	4	4	4	3	4	4	39	
57	4	4	4	4	3	2	2	4	5	5	37	
58	4	3	4	3	3	3	3	4	4	4	35	
59	4	4	4	4	4	4	4	2	3	4	37	
60	5	5	5	5	5	5	5	5	5	5	50	
61	4	4	5	5	4	5	4	4	4	5	44	
62	4	4	4	4	4	4	4	4	4	4	40	
63	5	5	5	5	5	5	5	5	5	5	50	
64	4	4	4	4	4	4	4	4	4	4	40	
65	4	4	4	4	4	4	4	5	4	4	41	
66	2	4	3	1	2	2	3	4	4	4	29	

67	4	4	4	4	4	4	4	4	4	4	4	40
68	4	4	4	4	4	5	4	4	4	4	4	41
69	4	4	4	4	4	4	4	4	4	4	4	40
70	4	4	4	5	4	4	4	4	4	4	5	42
71	4	4	4	4	4	5	5	5	4	5	5	44
72	4	4	4	4	4	4	4	4	4	4	4	40

Resp	Jawaban Pertanyaan Variabel Y (<i>Cyber Crime</i>)										Total
	1	2	3	4	5	6	7	8	9	10	
1	2	2	3	1	1	1	2	1	1	3	17
2	1	1	1	1	1	5	5	5	5	5	30
3	2	2	3	2	4	4	4	4	4	4	33
4	1	1	1	1	1	4	1	1	4	3	18
5	2	2	2	2	2	4	4	4	4	3	29
6	2	2	2	2	2	2	2	2	3	3	22
7	3	3	3	3	3	3	3	3	3	3	30

8	1	1	1	1	1	4	4	4	4	4	25
9	1	1	1	1	1	4	4	3	4	3	23
10	1	1	4	1	4	4	4	4	2	4	29
11	1	1	1	4	3	3	3	3	1	3	23
12	2	2	2	3	3	3	3	3	4	2	27
13	1	1	1	4	4	3	4	1	1	1	21
14	2	2	3	3	3	3	3	3	1	3	26
15	3	3	2	1	4	4	5	5	5	5	37
16	2	2	3	2	4	4	4	4	3	3	31
17	4	2	2	3	4	4	4	4	3	4	34
18	1	1	3	1	3	3	3	2	1	2	20
19	2	1	3	3	4	4	4	2	4	3	30
20	1	1	5	4	4	4	4	3	4	4	34
21	2	2	2	2	2	4	4	4	4	4	30
22	1	1	1	1	1	1	1	1	1	1	10
23	2	2	2	3	3	3	3	2	3	3	26

24	1	1	3	1	3	4	4	3	2	4	26
25	1	1	5	4	4	5	5	5	5	4	39
26	3	2	5	4	4	4	4	3	3	3	35
27	3	3	3	4	3	3	3	3	1	3	29
28	2	2	3	2	3	4	4	3	3	3	29
29	1	1	2	1	3	3	3	3	3	1	21
30	4	3	5	3	4	4	4	3	2	2	34
31	1	1	4	4	4	4	4	4	3	3	32
32	1	1	1	1	1	4	4	3	4	3	23
33	3	3	4	3	4	4	4	4	4	4	37
34	2	2	2	2	4	4	4	4	4	4	32
35	2	2	4	3	5	5	5	5	5	5	41
36	1	1	5	3	5	4	4	4	5	4	36
37	4	4	4	3	5	4	4	4	4	4	40
38	1	1	3	1	1	4	5	4	4	4	28
39	2	2	4	2	4	4	4	4	4	4	34

40	4	4	5	5	5	5	5	5	5	5	5	48
41	4	4	3	4	4	4	4	4	4	4	4	39
42	1	1	1	1	1	4	4	3	3	3	3	22
43	2	2	4	3	4	4	4	4	3	4	4	34
44	2	2	2	2	2	5	4	4	4	4	4	31
45	1	2	3	2	3	4	3	3	3	3	3	27
46	5	5	5	1	5	5	5	5	5	5	5	46
47	2	2	3	3	3	3	3	3	3	3	3	28
48	4	4	4	4	4	4	4	4	4	4	4	40
49	2	2	3	2	2	2	3	3	3	2	2	24
50	1	1	1	1	1	1	4	5	5	5	5	25
51	2	2	2	2	2	2	2	4	4	3	3	25
52	3	2	5	5	5	5	5	5	1	4	4	40
53	1	1	3	3	3	3	4	4	4	1	1	27
54	3	3	2	4	3	4	3	3	2	4	4	31
55	2	2	4	3	4	4	4	3	3	4	4	33

56	2	2	3	2	3	4	4	3	4	2	29
57	4	2	5	5	5	5	5	5	4	5	45
58	2	2	2	2	4	4	5	3	3	4	31
59	2	2	2	3	3	3	3	2	3	2	25
60	5	5	5	1	5	5	5	5	5	5	46
61	4	4	4	5	5	5	5	5	5	4	46
62	2	2	3	3	3	4	3	2	1	2	25
63	1	1	4	1	5	5	5	2	4	5	33
64	2	2	4	2	4	4	4	4	3	4	33
65	3	3	4	3	4	4	4	4	4	4	37
66	2	2	2	3	3	4	4	4	3	2	29
67	4	4	4	5	5	4	4	4	3	3	40
68	2	2	2	2	2	4	4	4	4	4	30
69	2	2	2	2	2	4	4	4	3	4	29
70	4	4	5	4	4	4	4	4	4	4	41
71	1	1	4	2	4	4	4	4	4	4	32

72		1		1		1		1		4		4		4		3		4		24
----	--	---	--	---	--	---	--	---	--	---	--	---	--	---	--	---	--	---	--	----

Lampiran 2

UJI VALIDITAS DAN RELIABILITAS

Variabel X1 (Penggunaan <i>Internet Banking</i>)			
Butir	r hitung	r tabel	Keterangan
1.	.789 **	0,235	Valid
2.	.745 **	0,235	Valid
3.	.760 **	0,235	Valid
4.	.751 **	0,235	Valid
5.	.627 **	0,235	Valid
6.	.764 **	0,235	Valid
7.	.840 **	0,235	Valid
8.	.828 **	0,235	Valid
9.	.718 **	0,235	Valid
10.	.662 **	0,235	Valid

Variabel X2 (<i>Client Charter</i>)			
Butir	r hitung	r tabel	Keterangan
1	.645 **	0,235	Valid
2	.760 **	0,235	Valid
3	.726 **	0,235	Valid
4	.545 **	0,235	Valid
5	.755 **	0,235	Valid
6	.656 **	0,235	Valid
7	.681 **	0,235	Valid
8	.756 **	0,235	Valid
9	.577 **	0,235	Valid
10	.497 **	0,235	Valid

Variabel X3 (Kerahasiaan Data Nasabah)			
Butir	r hitung	r tabel	Keterangan
1	.630 **	0,235	Valid
2	.482 **	0,235	Valid
3	.483 **	0,235	Valid
4	.763 **	0,235	Valid
5	.572 **	0,235	Valid
6	.659 **	0,235	Valid
7	.416 **	0,235	Valid
8	.596 **	0,235	Valid
9	.704 **	0,235	Valid
10	.581 **	0,235	Valid

Variabel X4 (<i>Test and Trial Drive</i>)			
Butir	r hitung	r tabel	Keterangan
1	.670 **	0,235	Valid
2	.664 **	0,235	Valid
3	.654 **	0,235	Valid
4	.779 **	0,235	Valid
5	.637 **	0,235	Valid
6	.621 **	0,235	Valid
7	.737 **	0,235	Valid
8	.726 **	0,235	Valid
9	.756 **	0,235	Valid
10	.619 **	0,235	Valid

Variabel X5 (<i>Customer Support Service</i>)				Variabel Y (<i>Cyber Crime</i>)			
Butir	r hitung	r tabel	Keterangan	Butir	r hitung	r tabel	Keterangan
1	.764 **	0,235	Valid	1	.727 **	0,235	Valid
2	.601 **	0,235	Valid	2	.681 **	0,235	Valid
3	.736 **	0,235	Valid	3	.746 **	0,235	Valid
4	.815 **	0,235	Valid	4	.524 **	0,235	Valid
5	.789 **	0,235	Valid	5	.783 **	0,235	Valid
6	.712 **	0,235	Valid	6	.700 **	0,235	Valid
7	.695 **	0,235	Valid	7	.723 **	0,235	Valid
8	.632 **	0,235	Valid	8	.731 **	0,235	Valid
9	.534 **	0,235	Valid	9	.527 **	0,235	Valid
10	.610 **	0,235	Valid	10	.647 **	0,235	Valid

Estimasi Reliabilitas

Variabel	Koefisien Reliabilitas	Interpretasi
Penggunaan <i>Internet Banking</i> (X1)	0,910	Sangat Tinggi
<i>Client Charter</i> (X2)	0,848	Sangat Tinggi
Kerahasiaan Data Nasabah (X3)	0,780	Tinggi
<i>Test and Trial Drive</i> (X4)	0,875	Sangat Tinggi
<i>Customer Support Service</i> (X5)	0,873	Sangat Tinggi
<i>Cyber Crime</i> (Y)	0,865	Sangat Tinggi

Lampiran 3.

UJI PRASYARAT ANALISIS

Uji Normalitas

Uji Linearitas

Uji Multikoleniaritas

Uji Heteroskedastisitas

UJI NORMALITAS

One-Sample Kolmogorov-Smirnov Test

		Residual
N		72
Normal Parameters ^{a,,b}	Mean	.0000
	Std. Deviation	6.40624
Most Extreme Differences	Absolute	.057
	Positive	.052
	Negative	-.057
Kolmogorov-Smirnov Z		.481
Asymp. Sig. (2-tailed)		.975

a. Test distribution is Normal.

b. Calculated from data.

UJI LINEARITAS

ANOVA Table

		Sum of Squares	df	Mean Square	F	Sig.
Cyber Crime * Penggunaan IB	Between Groups (Combined)	1358.340	24	56.597	1.025	.458
	Linearity	297.802	1	297.802	5.391	.025
	Deviation from Linearity	1060.538	23	46.110	.835	.674
	Within Groups	2596.105	47	55.236		
Total		3954.444	71			

ANOVA Table

		Sum of Squares	df	Mean Square	F	Sig.
Cyber Crime * Client Charter	Between Groups (Combined)	1157.928	16	72.370	1.423	.165
	Linearity	44.502	1	44.502	.875	.354
	Deviation from Linearity	1113.426	15	74.228	1.460	.154
	Within Groups	2796.517	55	50.846		
	Total	3954.444	71			

ANOVA Table

		Sum of Squares	df	Mean Square	F	Sig.
Cyber Crime * Kerahasiaan Data Nasabah	Between Groups (Combined)	1408.748	16	88.047	1.902	.040
	Linearity	466.617	1	466.617	10.081	.002
	Deviation from Linearity	942.131	15	62.809	1.357	.202
	Within Groups	2545.696	55	46.285		
	Total	3954.444	71			

ANOVA Table

		Sum of Squares	df	Mean Square	F	Sig.
Cyber Crime * Test n Trial Drive	Between Groups (Combined)	1210.188	18	67.233	1.298	.227
	Linearity	263.593	1	263.593	5.091	.028
	Deviation from Linearity	946.596	17	55.682	1.075	.401
	Within Groups	2744.256	53	51.778		
	Total	3954.444	71			

ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
Cyber Crime * Customer Service	Between Groups	(Combined)	1465.206	19	77.116	1.611	.089
		Linearity	448.150	1	448.150	9.362	.003
		Deviation from Linearity	1017.056	18	56.503	1.180	.311
	Within Groups		2489.238	52	47.870		
		Total	3954.444	71			

UJI MULTIKOLENIARITAS**Coefficients^a**

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.	Collinearity Statistics	
		B	Std. Error				Tolerance	VIF
1	(Constant)	-2.911	9.578		-.304	.762		
	Penggunaan IB	.281	.132	.252	2.124	.037	.795	1.259
	Client Charter	-.591	.253	-.331	-2.341	.022	.559	1.790
	Kerahasiaan Data Nasabah	.630	.250	.348	2.518	.014	.583	1.715
	Test n Trial Drive	.036	.194	.025	.187	.852	.629	1.591
	Customer Service	.528	.210	.306	2.514	.014	.753	1.328

a. Dependent Variable: Cyber Crime

UJI HETEROSKEDASTISITAS

Coefficients^a

Model	Unstandardized Coefficients			T	Sig.	Collinearity Statistics	
	B	Std. Error	Beta			Tolerance	VIF
1 (Constant)	-1.287	5.860		-.220	.827		
Penggunaan IB	.003	.081	.005	.035	.972	.795	1.259
Client Charter	.075	.154	.079	.484	.630	.559	1.790
Kerahasiaan Data Nasabah	.075	.153	.078	.490	.625	.583	1.715
Test n Trial Drive	-.025	.119	-.032	-.211	.834	.629	1.591
Customer Service	.031	.128	.034	.244	.808	.753	1.328

a. Dependent Variable: RES2

Lampiran 4.

HASIL ANALISIS DATA

Hasil Regresi Ganda

Output Analisis Uji Determinasi

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.513 ^a	.263	.207	6.64448

a. Predictors: (Constant), Customer Service , Penggunaan IB, Kerahasiaan Data Nasabah, Test n Trial Drive, Client Charter

Output Analisis Uji F

ANOVA^b

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1040.607	5	208.121	4.714	.001 ^a
	Residual	2913.837	66	44.149		
	Total	3954.444	71			

a. Predictors: (Constant), Customer Service , Penggunaan IB, Kerahasiaan Data Nasabah, Test n Trial Drive, Client Charter

b. Dependent Variable: Cyber Crime

Output Analisis Uji T

Coefficients^a

Model		Unstandardized Coefficients		Beta	t	Sig.
		B	Std. Error			
1	(Constant)	-2.911	9.578		-.304	.762
	Penggunaan IB	.281	.132	.252	2.124	.037
	Client Charter	-.591	.253	-.331	-2.341	.022
	Kerahasiaan Data Nasabah	.630	.250	.348	2.518	.014
	Test n Trial Drive	.036	.194	.025	.187	.852
	Customer Service	.528	.210	.306	2.514	.014

a. Dependent Variable: Cyber Crime

Lampiran 5.

PERHITUNGAN DISTRIBUSI FREKUENSI

a. Menentukan Tabel Distribusi Frekuensi Data Penggunaan *Internet Banking*

1) Menentukan Jumlah Kelas Interval

$$\begin{aligned}K &= 1 + 3,3 \log 72 \\&= 1 + 3,3 (1,85) \\&= 1 + 6,129 \\&= 7,129 \\&= 8\end{aligned}$$

2) Menentukan Rentang Data

$$\begin{aligned}\text{Rentang Data} &= \text{Nilai Maksimum} - \text{Nilai Minimum} \\&= 50 - 11 \\&= 39\end{aligned}$$

3) Menentukan Panjang Kelas

$$\begin{aligned}\text{Panjang Kelas} &= \text{Rentang Data} / \text{Jumlah Kelas} \\&= 39/8 \\&= 4,87 \\&= 5\end{aligned}$$

4) Menghitung Distribusi Kecenderungan Variabel

$$\begin{aligned}\text{Mean Ideal (Mi)} &= \frac{1}{2} (\text{X max} + \text{X min}) \\&= \frac{1}{2} (50 + 10) \\&= \frac{1}{2} (60) \\&= 30\end{aligned}$$

$$\begin{aligned}\text{Standar Deviasi Ideal (SDi)} &= 1/6 (\text{X max} - \text{X min}) \\&= 1/6 (50 - 10) \\&= 1/6 (40) \\&= 6,67 \\&= 7\end{aligned}$$

Penentuan Kategori:

a) Rendah = $\{ Mi - 1 (SDi) \}$
= $\{ 30 - 1 (7) \}$
= < 23

b) Sedang = $\{ Mi - 1 (SDi) \}$ s/d $\{ Mi + 1 (SDi) \}$
= $\{ 30 - 1 (7) \}$ s/d $\{ 30 + 1 (7) \}$
= 23 s/d 37

c) Tinggi = $\{ Mi + 1 (SDi) \}$
= $\{ 30 + 1 (7) \}$
= > 37

b. Menentukan Tabel Distribusi Frekuensi Data *Client Charter*

1) Menentukan Jumlah Kelas Interval

$$\begin{aligned}K &= 1 + 3,3 \log 72 \\&= 1 + 3,3 (1,85) \\&= 1 + 6,129 \\&= 7,129 \\&= 8\end{aligned}$$

2) Menentukan Rentang Data

$$\begin{aligned}
 \text{Rentang Data} &= \text{Nilai Maksimum} - \text{Nilai Minimum} \\
 &= 50 - 31 \\
 &= 19
 \end{aligned}$$

3) Menentukan Panjang Kelas

$$\begin{aligned}
 \text{Panjang Kelas} &= \text{Rentang Data}/\text{Jumlah Kelas} \\
 &= 19/8 \\
 &= 2,37 \\
 &= 3
 \end{aligned}$$

4) Menghitung Distribusi Kecenderungan Variabel

$$\begin{aligned}
 \text{Mean Ideal (Mi)} &= \frac{1}{2} (\text{X max} + \text{X min}) \\
 &= \frac{1}{2} (50 + 10) \\
 &= \frac{1}{2} (60) \\
 &= 30
 \end{aligned}$$

$$\text{Standar Deviasi Ideal (SDi)} = 1/6 (\text{X max} - \text{X min})$$

$$\begin{aligned}
 &= 1/6 (50 - 10) \\
 &= 1/6 (40) \\
 &= 6,67 \\
 &= 7
 \end{aligned}$$

Penentuan Kategori:

$$\begin{aligned}
 \text{a) Rendah} &= < \{ \text{Mi} - 1 (\text{SDi}) \} \\
 &= < \{ 30 - 1 (7) \} \\
 &= < 23 \\
 \text{b) Sedang} &= \{ \text{Mi} - 1 (\text{SDi}) \} \text{ s/d } \{ \text{Mi} + 1 (\text{SDi}) \} \\
 &= \{ 30 - 1 (7) \} \text{ s/d } \{ 30 + 1 (7) \} \\
 &= 23 \text{ s/d } 37 \\
 \text{c) Tinggi} &= > \{ \text{Mi} + 1 (\text{SDi}) \} \\
 &= > \{ 30 + 1 (7) \} \\
 &= > 37
 \end{aligned}$$

c. Menentukan Tabel Distribusi Frekuensi Data Kerahasiaan Data Nasabah

1) Menentukan Jumlah Kelas Interval

$$\begin{aligned}
 \text{K} &= 1 + 3,3 \log 72 \\
 &= 1 + 3,3 (1,85) \\
 &= 1 + 6,129 \\
 &= 7,129 \\
 &= 8
 \end{aligned}$$

2) Menentukan Rentang Data

$$\begin{aligned}
 \text{Rentang Data} &= \text{Nilai Maksimum} - \text{Nilai Minimum} \\
 &= 50 - 30 \\
 &= 20
 \end{aligned}$$

3) Menentukan Panjang Kelas

$$\begin{aligned}
 \text{Panjang Kelas} &= \text{Rentang Data}/\text{Jumlah Kelas} \\
 &= 20/8 \\
 &= 2,5 \\
 &= 3
 \end{aligned}$$

4) Menghitung Distribusi Kecenderungan Variabel

$$\begin{aligned}
 \text{Mean Ideal (Mi)} &= \frac{1}{2} (\text{X max} + \text{X min}) \\
 &= \frac{1}{2} (50 + 10) \\
 &= \frac{1}{2} (60) \\
 &= 30
 \end{aligned}$$

$$\text{Standar Deviasi Ideal (SDi)} = \frac{1}{6} (\text{X max} - \text{X min})$$

$$\begin{aligned}
 &= \frac{1}{6} (50 - 10) \\
 &= \frac{1}{6} (40) \\
 &= 6,67 \\
 &= 7
 \end{aligned}$$

Penentuan Kategori:

- a) Rendah = $\{ \text{Mi} - 1 (\text{SDi}) \}$
 $= \{ 30 - 1 (7) \}$
 $= < 23$
- b) Sedang = $\{ \text{Mi} - 1 (\text{SDi}) \} \text{ s/d } \{ \text{Mi} + 1 (\text{SDi}) \}$
 $= \{ 30 - 1 (7) \} \text{ s/d } \{ 30 + 1 (7) \}$
 $= 23 \text{ s/d } 37$
- c) Tinggi = $\{ \text{Mi} + 1 (\text{SDi}) \}$
 $= \{ 30 + 1 (7) \}$
 $= > 37$

d. Menentukan Tabel Distribusi Frekuensi Data *Test and Trial Drive*

1) Menentukan Jumlah Kelas Interval

$$\begin{aligned}
 K &= 1 + 3,3 \log 72 \\
 &= 1 + 3,3 (1,85) \\
 &= 1 + 6,129 \\
 &= 7,129 \\
 &= 8
 \end{aligned}$$

2) Menentukan Rentang Data

$$\begin{aligned}
 \text{Rentang Data} &= \text{Nilai Maksimum} - \text{Nilai Minimum} \\
 &= 50 - 28 \\
 &= 22
 \end{aligned}$$

3) Menentukan Panjang Kelas

$$\begin{aligned}
 \text{Panjang Kelas} &= \text{Rentang Data}/\text{Jumlah Kelas} \\
 &= 22/8 \\
 &= 2,75 \\
 &= 3
 \end{aligned}$$

4) Menghitung Kecenderungan Variabel

$$\begin{aligned}
 \text{Mean Ideal (Mi)} &= \frac{1}{2} (\text{X max} + \text{X min}) \\
 &= \frac{1}{2} (50 + 10) \\
 &= \frac{1}{2} (60) \\
 &= 30
 \end{aligned}$$

$$\text{Standar Deviasi Ideal (SDi)} = \frac{1}{6} (\text{X max} - \text{X min})$$

$$\begin{aligned}
 &= \frac{1}{6} (50 - 10) \\
 &= \frac{1}{6} (40)
 \end{aligned}$$

$$= 6,67 \\ = 7$$

Penentuan Kategori:

- a) Rendah = $\{Mi - 1 (SDi)\}$
 $= \{30 - 1 (7)\}$
 $= < 23$
- b) Sedang = $\{Mi - 1 (SDi)\} \text{ s/d } \{Mi + 1 (SDi)\}$
 $= \{30 - 1 (7)\} \text{ s/d } \{30 + 1 (7)\}$
 $= 23 \text{ s/d } 37$
- c) Tinggi = $\{Mi + 1 (SDi)\}$
 $= \{30 + 1 (7)\}$
 $= > 37$

e. Menentukan Tabel Distribusi Frekuensi Data *Customer Support Service*

1) Menentukan Jumlah Kelas Interval

$$K = 1 + 3,3 \log 72 \\ = 1 + 3,3 (1,85) \\ = 1 + 6,129 \\ = 7,129 \\ = 8$$

2) Menentukan Rentang Data

$$\text{Rentang Data} = \text{Nilai Maksimum} - \text{Nilai Minimum} \\ = 50 - 29 \\ = 21$$

3) Menentukan Panjang Kelas

$$\text{Panjang Kelas} = \text{Rentang Data}/\text{Jumlah Kelas} \\ = 21/8 \\ = 2,625 \\ = 3$$

4) Menentukan Distribusi Kecenderungan Variabel

$$\text{Mean Ideal (Mi)} = \frac{1}{2} (\text{X max} + \text{X min}) \\ = \frac{1}{2} (50 + 10) \\ = \frac{1}{2} (60) \\ = 30$$

Standar Deviasi Ideal (SDi) = $1/6 (\text{X max} - \text{X min})$

$$= 1/6 (50 - 10) \\ = 1/6 (40) \\ = 6,67 \\ = 7$$

Penentuan Kategori:

- a) Rendah = $\{Mi - 1 (SDi)\}$
 $= \{30 - 1 (7)\}$
 $= < 23$
- b) Sedang = $\{Mi - 1 (SDi)\} \text{ s/d } \{Mi + 1 (SDi)\}$
 $= \{30 - 1 (7)\} \text{ s/d } \{30 + 1 (7)\}$
 $= 23 \text{ s/d } 37$

$$\begin{aligned}
 c) \text{ Tinggi} &=> \{M_i + 1 (SD_i)\} \\
 &=> \{30 + 1 (7)\} \\
 &=> 37
 \end{aligned}$$

f. Menentukan Tabel Distribusi Frekuensi Data *Cyber Crime*

1) Menentukan Jumlah Kelas Interval

$$\begin{aligned}
 K &= 1 + 3,3 \log 72 \\
 &= 1 + 3,3 (1,85) \\
 &= 1 + 6,129 \\
 &= 7,129 \\
 &= 8
 \end{aligned}$$

2) Menentukan Rentang Data

$$\begin{aligned}
 \text{Rentang Data} &= \text{Nilai Maksimum} - \text{Nilai Minimum} \\
 &= 48 - 10 \\
 &= 38
 \end{aligned}$$

3) Menentukan Panjang Kelas

$$\begin{aligned}
 \text{Panjang Kelas} &= \text{Rentang Data}/\text{Jumlah Kelas} \\
 &= 38/8 \\
 &= 4,75 \\
 &= 5
 \end{aligned}$$

4) Menghitung Distribusi Kecenderungan Variabel

$$\begin{aligned}
 \text{Mean Ideal (M_i)} &= \frac{1}{2} (\text{X max} + \text{X min}) \\
 &= \frac{1}{2} (50 + 10) \\
 &= \frac{1}{2} (60) \\
 &= 30
 \end{aligned}$$

$$\text{Standar Deviasi Ideal (SD_i)} = \frac{1}{6} (\text{X max} - \text{X min})$$

$$\begin{aligned}
 &= \frac{1}{6} (50 - 10) \\
 &= \frac{1}{6} (40) \\
 &= 6,67 \\
 &= 7
 \end{aligned}$$

Penentuan Kategori:

- a) Rendah = < {M_i - 1 (SD_i)}

$$\begin{aligned}
 &=< \{30 - 1 (7)\} \\
 &=< 23
 \end{aligned}$$
- b) Sedang = {M_i - 1 (SD_i)} s/d {M_i + 1 (SD_i)}

$$\begin{aligned}
 &= \{30 - 1 (7)\} \text{ s/d } \{30 + 1 (7)\} \\
 &= 23 \text{ s/d } 37
 \end{aligned}$$
- c) Tinggi = > {M_i + 1 (SD_i)}

$$\begin{aligned}
 &=> \{30 + 1 (7)\} \\
 &=> 37
 \end{aligned}$$

Lampiran 6.

PERHITUNGAN SUMBANGAN RELATIF DAN SUMBANGAN EFEKTIF

Sumbangan Relatif dan Sumbangan Efektif

Variabel	Koefisien Regresi (Beta)	Koefisien Korelasi (r)	R _{square}
X1	0,252	0,274	0,263
X2	0,331	0,106	
X3	0,348	0,344	
X4	0,025	0,258	
X5	0,306	0,337	

$$\mathbf{SE(X)\% = Beta_x \times r_{xy} \times 100\%}$$

$$\mathbf{SE(X1)\% = 0,252 \times 0,274 \times 100\% = 6,90\%}$$

$$\mathbf{SE(X2)\% = 0,331 \times 0,106 \times 100\% = 3,50\%}$$

$$\mathbf{SE(X3)\% = 0,348 \times 0,344 \times 100\% = 11,97\%}$$

$$\mathbf{SE(X4)\% = 0,025 \times 0,258 \times 100\% = 0,64\%}$$

$$\mathbf{SE(X5)\% = 0,306 \times 0,337 \times 100\% = 10,31\%}$$

$$\mathbf{SE \text{ total} = 6,90\% - 3,50\% + 11,97\% + 0,64\% + 10,31\% = 26,32\%}$$

$$\mathbf{SR(X)\% = \frac{SE(X)\%}{R^2}}$$

$$\mathbf{SR(X1)\% = 6,90/0,263 = 26,23\%}$$

$$\mathbf{SR(X2)\% = 3,50/0,263 = 13,30\%}$$

$$\mathbf{SR(X3)\% = 11,97/0,263 = 45,51\%}$$

$$\mathbf{SR(X4)\% = 0,64/0,263 = 2,43\%}$$

$$\mathbf{SR(X5)\% = 10,31/0,263 = 39,20\%}$$

$$\mathbf{SR \text{ total} = 26,23\% - 13,30\% + 45,51\% + 2,43\% + 39,20\% = 100\%}$$