International Journal of Emerging Trends in Social Sciences
ISSN: 2521-3539
Vol. 13, No. 2, pp. 22-32, 2022
DOI: 10.55217/103.v13i2.563

Cyber Crime Fraud in Jakarta and Tangerang

Zakkiandri[1]
Karsam[2]
Budiandru[3]♣

[1,2]*STIE Swadaya, Indonesia.*
[1]*Email:* zakkiandri@gmail.com
[2]*Email:* karsamse86@gmail.com
[3]*University of Muhammadiyah Prof. Dr. HAMKA, Jakarta, Indonesia.*
[3]*Email:* budiandru@uhamka.ac.id

Abstract

The purpose of this study is to determine Cyber Security, Cyber Hardware, Information Systems against Fraud. The population of this study are users of information technology in Jakarta and Tangerang. This research method is a qualitative method and the type of primary data by collecting questionnaires. Types of primary data are data taken directly from the object of research, using a questionnaire with a total of 103 respondents. While secondary data is data obtained from documents from banks and other sources related to this research. The sampling technique is the analysis of the outer model (measurement model) and analysis of the inner model (structural model) using the Multivariate Structural Equation Model (SEM) Partial least square or commonly abbreviated as PLS is a type of statistical analysis whose use is similar to SEM in covariance analysis. Because it is similar to SEM, the basic framework in PLS used is based on linear regression. So, what is in linear regression, is also in PLS. It's just that it is given a different symbol, symbol or term. In participatory technique, the results of this study show that cybersecurity, cyber hardware has a positive effect on fraud. The performance of this research shows that Cyber security and cyber-Hardware have an effect on Fraud, so that users or users are more careful in using information technology and always update it. Simultaneously, the R-Square value is 0.257 or 25%, which means cyber security, cyber hardware influenced by the information system against fraud by 25%.

Keywords:
Cyber hardware
Cyber security
Fraud
Information systems.

Publisher:
Scientific Publishing Institute

Received: *8 August 2022*
Revised: *4 October 2022*
Accepted: *19 October 2022*
Published: *1 November 2022*

(♣ Corresponding Author)

Funding: This study received no specific financial support.
Competing Interests: The authors declare that they have no competing interests.

1. Introduction

Rapidly increasing information technology causes very significant social, economic and cultural changes (Fahlevi, Saparudin, Maemunah, & Irma, 2019) and provides the same benefits and impacts depending on the users of the information technology (Anggono & Riskiyadi, 2021). The positive benefits that can be obtained from information technology are that it makes it easier for individuals or groups to carry out their activities, while the negative impacts arise due to the misuse of technology by individuals or groups for cybercrime that can harm others (Gani, 2014).

Rapid technological advances are also accompanied by increasing security systems as a response to the drastic increase in cybercrime actions (Peters, Shevchenko, & Cohen, 2018). As a result, cybercrime actors are always more active and quick to make new breakthroughs on the security system established by anti-cybercrime or better known as cybersecurity. A very worrying condition occurs when the perpetrators of cybercrime are also experts in anti-cybercrime actions, so that the new mode of cybercrime is difficult to detect and solve with cybersecurity. Cybercrime attacks that continue to grow rapidly but cybersecurity stagnates are a problem that must be solved immediately (Anggono & Riskiyadi, 2021).

Losses from cybercrime are difficult to estimate and verify because in addition to financial losses, other losses due to damage, loss or leakage of private data cause a decline in the reputation of a company). As a result of cybercrime attacks, all countries in the world are affected, especially for countries that are still in the developing stage in the field of information and communication technology, which is marked by a drastic increase in cybercrime levels. Anticipatory steps must be taken by the government to prevent cybercrime, which is meant by establishing and implementing regulations on cybercrime and encouraging the private sector to contribute to the fight against cybercrime by strengthening cybersecurity (Falco, 2019).

In the development of increasingly high digital transactions, it brings complex implications in human life and relations between countries (Lana, 2021). When we talk about high-tech crimes such as Internet crime or cybercrime, it is as if the law is behind the scenes (Kaur & Ramkumar, 2021). With the growing use of the Internet, computer-savvy people for a specific purpose can use computers and the Internet to commit crimes or "pranks" that harm others.

The development of information and communication technology has spawned many breakthroughs, one of which is the developing information system for payment technology, fund transfers, remittances or fund transfers from abroad, lending or lending, crowdfunding or crowdfunding, financial intermediation or intermediaries, retail investment, financial planning, financial research and other financial services (Das, 2019).

This study aims to identify the studies that have been carried out so far and provide an overview of the development of cybercrime, cybersecurity, information systems against fraud. This research was conducted by selecting, collecting, extracting and analyzing articles in accordance with the research questions in order to obtain results that cover all of the selected articles. The results of this study provide an overview of cybercrime and cybersecurity in fintech that can be used as a reference for theories, frameworks and research models so that they can be useful for increasing insight and knowledge about cybercrime challenges and cybersecurity anticipation, information systems against fraud and providing opportunities for future research.

Rapidly increasing information technology causes very significant social, economic and cultural changes (Fahlevi et al., 2019) and provides the same benefits and impacts depending on the users of the information technology (Anggono & Riskiyadi, 2021). The positive benefits that can be obtained from information technology are that it makes it easier for individuals or groups to carry out their activities, while the negative impacts arise due to the misuse of technology by individuals or groups for cybercrime that can harm others (Gani, 2014).

Rapid technological advances are also accompanied by increasing security systems as a response to the drastic increase in cybercrime actions (Peters et al., 2018). As a result, cybercrime actors are always more active and quick to make new breakthroughs on the security system established by anti-cybercrime or better known as cybersecurity. A very worrying condition occurs when the perpetrators of cybercrime are also experts in anti-cybercrime actions, so that the new mode of cybercrime is difficult to detect and solve with cybersecurity. Cybercrime attacks that continue to grow rapidly but cybersecurity stagnates are a problem that must be solved immediately (Anggono & Riskiyadi, 2021).

Losses from cybercrime are difficult to estimate and verify because in addition to financial losses, other losses due to damage, loss or leakage of private data cause a decline in the reputation of a company). As a result of cybercrime attacks, all countries in the world are affected, especially for countries that are still in the developing stage in the field of information and communication technology, which is marked by a drastic increase in cybercrime levels. Anticipatory steps must be taken by the government to prevent cybercrime, which is meant by establishing and implementing regulations on cybercrime and encouraging the private sector to contribute to the fight against cybercrime by strengthening cybersecurity (Falco, 2019).

In the development of increasingly high digital transactions, it brings complex implications in human life and relations between countries (Lana, 2021). When we talk about cybercrime and high-tech crimes like cybercrime, it is as if the law is behind the scenes (Kaur & Ramkumar, 2021). With the growing use of the Internet, computer-savvy people for a specific purpose can use computers and the Internet to commit crimes that harm others.

Cybercrime as a crime that occurs through or on a computer network on the internet (Sulisrudatin, 2014). But basically, the term cybercrime refers to an act of crime related to cyberspace (cyberspace) and actions that use computers. In simple terms, cybercrime is a term that refers to criminal activity in which a computer or computer network becomes a tool, target or place of crime (Hayati, 2021). This includes online auction fraud, check fraud, credit card fraud (carding), confidence fraud, identity fraud, child pornography, and others.

In Indonesia, regulations related to electronic information technology have been regulated in Law no. 11 of 2008 and Law no. 19 of 2016 regarding amendments to Law no. 11 of 2008 concerning Information and Electronic Transactions (Sadino & Dewi, 2016). In 2018, demonstrated that failure to use basic security measures to safeguard corporate data can leave organizations vulnerable to cyber-attacks (Hawamleh, Alorfi, Al-Gasawneh, & Al-Rawashdeh, 2020). Indonesia is listed as the country with the most cybercrime cases. Police Headquarters released losses from banking crime activities targeting the payment system in Indonesia.

Cybercrime is referred to as a form of criminal crime that arises because of the use of internet technology. For comparison, Forester and Morrison, computer experts from the United States describe that computer crime is a crime in which the tool/weapon used to commit the crime is a computer (Wang et al., 2021).

Figure 1 presentation on internet usage in Indonesia.

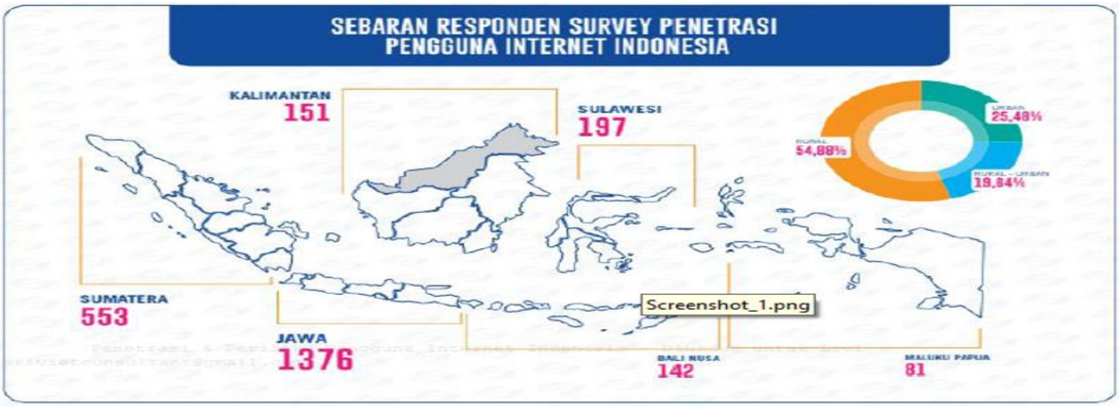

Figure 1. Data on internet usage in Indonesia.

Source: Fahlevi et al. (2019).

In Indonesia, internet users continue to grow, based on data from Relationship Index between (Indonesian Internet Service Providers Association) AIISP in 2018. The Association of Indonesian Internet Service Providers or abbreviated as AIISP is an association consisting of internet service providers which was formed at the First National Conference (MUNAS) on May 15, 1996 in Jakarta. The number of internet users in Indonesia in 2019 was 132.7 million users or about 51.5 percent of Indonesia's total population of 256.2 million. This is the most important part of the Indonesian population who use this internet technology. Where 65 percent of the island of Java or about 86.3 million people and the lowest in Maluku and Papua 2.5 percent, around 3.3 million people. The existence of cybercrime has become a threat to stability, so it is difficult for the government to balance the techniques of crime committed with computer technology, especially internet and intranet networks (Paterson, 2019). Cybersecurity is now considered an important part of individuals and families, as well as organizations, governments, educational institutions, and businesses. Proper learning about online behavior and system protection results in reduced vulnerabilities and a safer online environment (Zhang & Malacaria, 2021). *Cybercrime* based on conventional crimes as well as criminal acts and destruction of electronic media (Hamed, Sobhy, & Nassar, 2021). In 2018, the Police has handled more than 1,763 cyber crime cases. These include online auction fraud, check forgery, credit card or carding fraud, confidence fraud, and identity fraud (Security, 2014). The objectives of cyber attacks cover four areas, including:

a. Loss of integrity.
b. Loss of availability.
c. Loss of secrecy.
d. Physical destruction.
e. Cheating (Fraud).

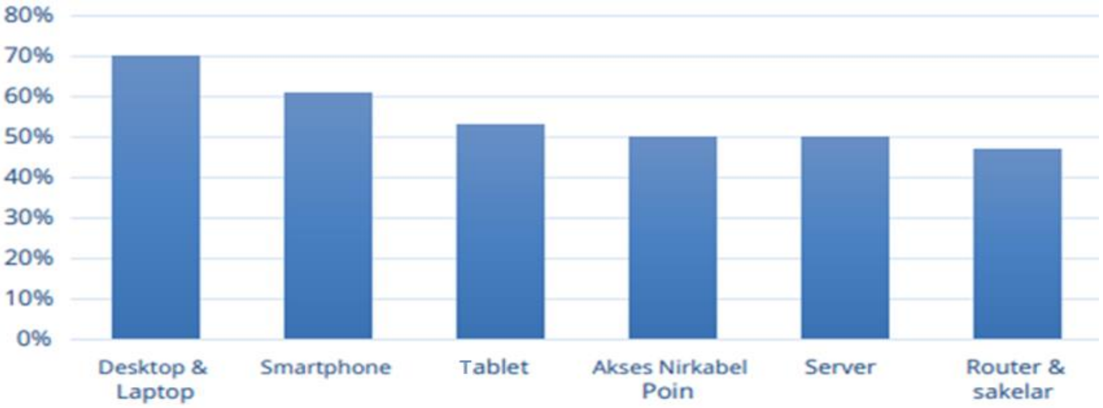

Figure 2. Security threat risk level.

Source: Figure 2 Security Threat Risk Level.

Based on the Figure 2, it has been noted that countries and companies have spent a lot of money on cybercrime activities. Millions of dollars have been lost through cybercrime activities. The researchers would like to use the statistical data below to show the modes of penetration of cybercrime in 2020.

In addition to threats from external companies, there are also possible security threats from internal companies with the potential for fraud. The forms of fraud can be various, even sometimes the fraud does not use technology alone but focuses more on profits to enrich oneself or a group in the form of changes in the presentation of financial statements (Thaifur, Maidin, Sidin, & Razak, 2021). Types of fraud based on group violations are:

a. Employee fraud (fraud), is fraud committed by employees in a working organization.

b. Management fraud (fraud), is a fraud committed by management using financial statements or fund transactions for various types of fraud, usually carried out to reduce the involvement of stakeholders in the organization.

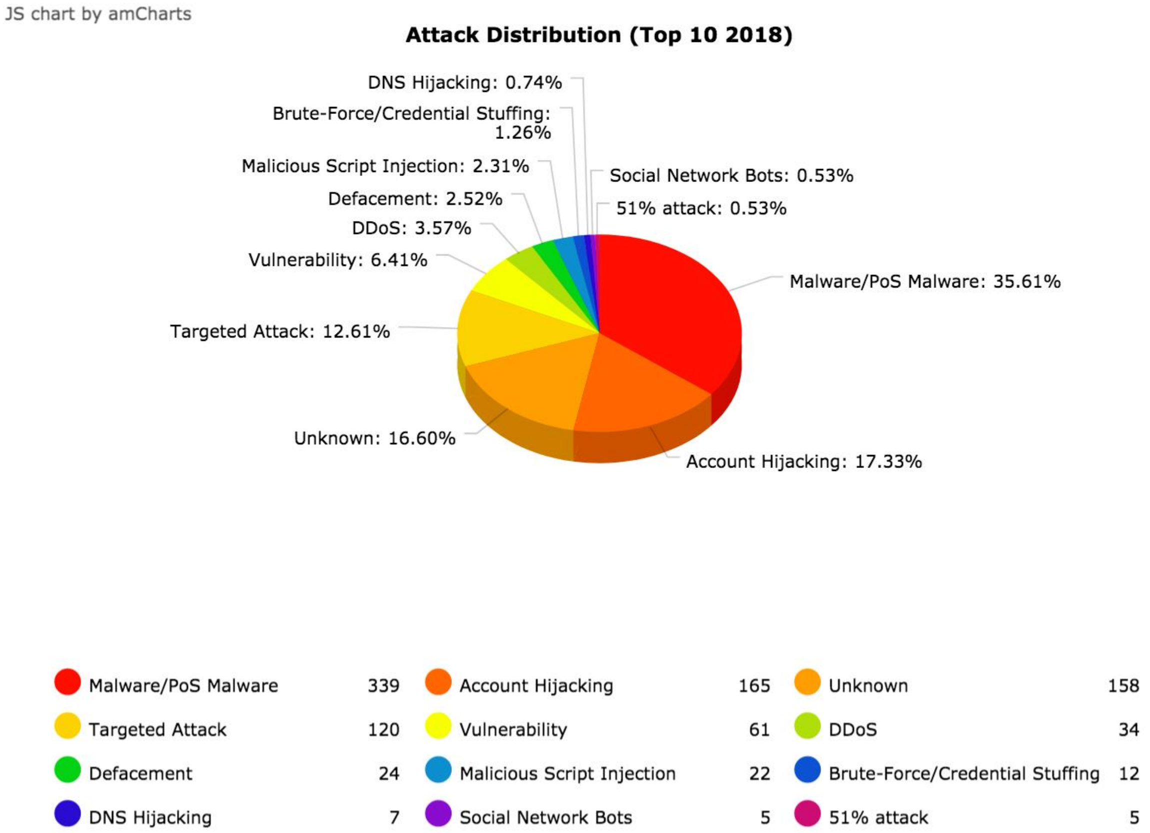

Figure 3. Cybercrime fraud rate.

Figure 3 Cybercrime Fraud Rate (Jain & Gupta, 2020).

The Figure 3 is the number of cybercrime frauds recorded during 2020.

2. Literature Review

2.1. Definition of Cyber Crime and Cyber Security

*Cybercrime*is a general term for crimes that attack computer systems or internet networks, with the aim of data theft, finance and distribution of malicious software code which is an illegal act in the field of information and communication technology as a modified form of conventional crime (Aravazhi, 2020). Cybercrime is an act carried out by perpetrators to destroy organizational networks by stealing valuable data, documents, hacking bank accounts and transferring them to their accounts.

To study these crimes, cybercriminology is needed which is a combination of knowledge from criminology, psychology, sociology, computer science, and cybersecurity to provide an in-depth understanding of cybercrime (Choi & Lee, 2018). Some of the main factors that cause cybercrime to develop rapidly are cybercrime tools, methods and media that are very easily accessible and learned on the internet, rapidly increasing technology improvements related to processing speed, data processing and analysis, internet bandwidth and other internet network activities as well as affordable access. manual to the source or server.

To study these crimes, cybercriminology is needed which is a combination of knowledge from criminology, psychology, sociology, computer science, and cybersecurity to provide an in-depth understanding of cybercrime (Choi & Lee, 2018). Some of the main factors that cause cybercrime to develop rapidly are cybercrime tools, methods and media that are very easily accessible and learned on the internet, rapidly increasing technology improvements related to processing speed, data processing and analysis, internet bandwidth and other internet network activities as well as affordable access. manual to the source or server.

In order to take anticipatory action to overcome cybercrime, cybersecurity is needed, namely protective measures against all forms of cybercrime attacks and recovery actions due to cybercrime. Cyber security is an action taken to protect computer systems from attacks or illegal access (Kaur & Ramkumar, 2021). Referring to the International Telecommunications Union (ITU), these cyber security measures include tools, policies, security concepts, etc., that can be used to protect organizations, and user assets (Zheng, Li, Xu, & Zhao, 2021).

2.2. Definition of Cyber Fraud

Meanwhile, fraud is a crime committed in a computer-based system or internet network that aims to manipulate financial information in order to make as much profit as possible (Mao, Sun, Zhu, & Li, 2022). Cyber fraud is a crime committed in a computer-based system or internet network that aims to manipulate financial information in order to make maximum profits (Hilal, Gadsden, & Yawney, 2022).

Various studies have stated that hacking, phishing and malware have an effect on cybersecurity compliance in the financial sector. Cybercrime perpetrators prefer to commit crimes in e-commerce and online payment systems because most personal information and credit card data are stored and processed in these applications (Aravazhi, 2020). Cybercrime is still very difficult to anticipate by e-commerce users so that it has the impact of decreasing user trust in e-commerce. Other research states that the development of e-commerce has been hampered due to lack of compliance with regulations, weak consumer protection against cybercrime. For this reason, both regulators and business players view that critical precautions must be taken and the application of the law must continue to follow the development of cybercrime (Fahlevi et al., 2019).

2.3. Types of Cyber Crime

2.3.1. Activity Based Cyber Crime

It can be seen that there are several types of cybercrime when viewed from its activities, namely as follows (Zheng et al., 2021):

a. Carding is shopping using someone else's credit card number and identity, obtained illegally, usually by stealing data on the internet. The term for the perpetrator is "carder" or it can also be called cyberfroud crime, aka fraud in cyberspace.

b. Hacking is breaking into computer programs belonging to other people/parties. Meanwhile, hackers are people who like to hack computers, and have the expertise to create and read certain programs and are obsessed with observing its security.

c. Cracking is a hacking for bad purposes. The term for "cracker" is "hacker" with a black hat (black hat hacker). In contrast to "carders" who only peek at credit cards, "crackers" peek at customers' deposits at various banks or other sensitive data centers for their own benefit. Even though they both break through other people's computer security, "hackers" are more focused on the process. While Cracker focus on enjoying the result.

d. Defacing is an activity to change the website pages of other parties, as happened on the websites of the Minister of Communication and Information and the Golkar Party, BI recently and the website during the 2004 general election comissions. There are deface actions that are purely for fun, to show off their skills, to show off their ability to make programs, but there are also malicious ones, to steal data and sell it to other parties.

e. Phishing is an activity to lure computer users on the internet (users) to want to provide information on the user's personal data (username) and password (password) on a website that has been defaced. Phising is usually intended for the online banking users. Fill in vital user data and passwords.

f. Spamming is the sending of unwanted news or advertisements via electronic mail (e-mail). Spam is often referred to as bulk e-mail or junk e-mail aka "junk".

g. Malware is a computer program that looks for weaknesses in software. Generally, malware is created to break into or damage a software or operating system. Malware consists of various kinds, namely: viruses, worms, Trojan horses, adware, browser hijackers and others.

2.3.2. Cyber Crime Crimes Based on the Operandi

Meanwhile, the types of cybercrime based on their modus operandi are:

1. *Unauthorized Access to Computer System and Service*, a crime committed by entering or infiltrating a computer network system illegally without permission or without the knowledge of the owner of the computer network system that it enters.
2. *Illegal Contents*, is a crime to enter data or information on the Internet about something that is not true, unethical, and can be considered unlawful or disturbing public order. For example, the posting of fake news or slander that will destroy the dignity or self-esteem of the other party.

3. Data Forgery is a crime by falsifying data on important documents stored as scripless documents via the Internet.
4. Cyber Espionage is a crime that utilizes the Internet network to carry out spying activities against other parties, by entering the computer network system of the target party.
5. Cyber Sabotage and Extortion, this crime is committed by disrupting, destroying or destroying data, computer programs or computer network systems connected to the Internet. Usually, this crime is carried out by infiltrating a logic bomb, computer virus or a certain program, so that data, computer programs or computer network systems cannot be used.
6. *Offense against Intellectual Property*, this crime is directed against intellectual property rights owned by others on the Internet. For example, illegal imitation of the appearance on a web page of another person's site, the broadcasting of information on the Internet that turns out to be someone else's trade secret, and so on.
7. *Infringements of Privacy:* This crime is usually directed against a person's personal information stored on a computerized personal data form which, if known by others, can harm the victim materially or immaterially, such as credit card numbers, ATM PIN numbers.

2.4. Characteristics of Cyber Crime

Based on some literature and practice, cybercrime has several distinctive characters compared to conventional crimes, namely (Garcia-Perez, Cegarra-Navarro, Sallos, Martinez-Caro, & Chinnaswamy, 2022):

a. an act that is carried out illegally, without such rights occurs in cyberspace, so it is difficult to ascertain which country's legal jurisdiction applies to it.
b. The act is carried out using any equipment that can be connected to the internet.
c. these actions result in material and immaterial losses (time, value, services, money, goods, self-esteem. dignity, confidentiality of information) which tend to be greater than conventional crimes.
d. the culprit is a person who controls the use of the internet and its applications.
e. these actions are often carried out transnationally / across national borders.

Crimes that are closely related to the use of technology based primarily on computers and telecommunications networks in some literature and practice can be grouped in several forms.

2.5. Computers as Targets for These Crimes Are Carried Out By Selected Criminal Groups

Unlike crimes that use computers as tools, these crimes require technical knowledge of the perpetrator. Thus, as technology develops, so does the nature of crime. This crime is relatively new in the history of computers, which explains how unprepared society and the world at large are to eradicate this crime. There are many crimes of this nature that are committed every day on the internet. Crimes that primarily target computer networks or devices include (Wall, 2008):

a. Computer viruses.
b. Denial-of-service attacks.
c. Malware (malicious code).
d. Etc.

2.6. Computers as Tools

If the individual is the main target of cybercrime, the computer can be considered as a tool rather than a target. These crimes generally lack technical expertise. Human weaknesses are generally exploited. The damage dealt is mostly psychological and intangible, making legal action against this variant more difficult. This is a crime that has existed for centuries in the offline world. Fraud, theft, and the like existed even before the development of high-tech equipment. The same criminals are simply given tools that increase their potential for victims and make them even more difficult to track down and catch. Other computer network crimes include:

a. Fraud and identity theft (although these are increasingly using hacking or phishing malware, making them examples of computer crime "as a target" and "computers as a tool").
b. Information war.
c. Phishing scam.
d. Spam.
e. Pornography, including harassment and threats. Sending email.

Sending unsolicited bulk email for commercial purposes (spam) is illegal in some jurisdictions. Phishing is mostly spread via email. Phishing emails may contain links to other websites that are affected by the malware. Alternatively, it may contain links to fake online banking or other websites used to steal personal account information.

3. Research Method

3.1. Research Design

This research method is a qualitative method and the type of primary data by collecting questionnaires. Types of primary data is data taken directly from the object of research, namely using a questionnaire. While secondary data is data obtained from documents from banks and other sources related to this research. The sampling technique is analysis of the outer model (measurement model) and analysis of the inner model (structural model) using the SmartPLS 3 Multivariate Structural Equation Model (SEM) technique.

The population in this study are users of information technology in Jakarta and Tangerang. The research was carried out in Jakarta and Tangerang. The research will be carried out from March 2022 to August 2022 with the consideration of getting more appropriate respondents.

4. Results and Discussion

4.1. Hypothesis Testing Results

Figure 4 presentation of measurement model / outside model.

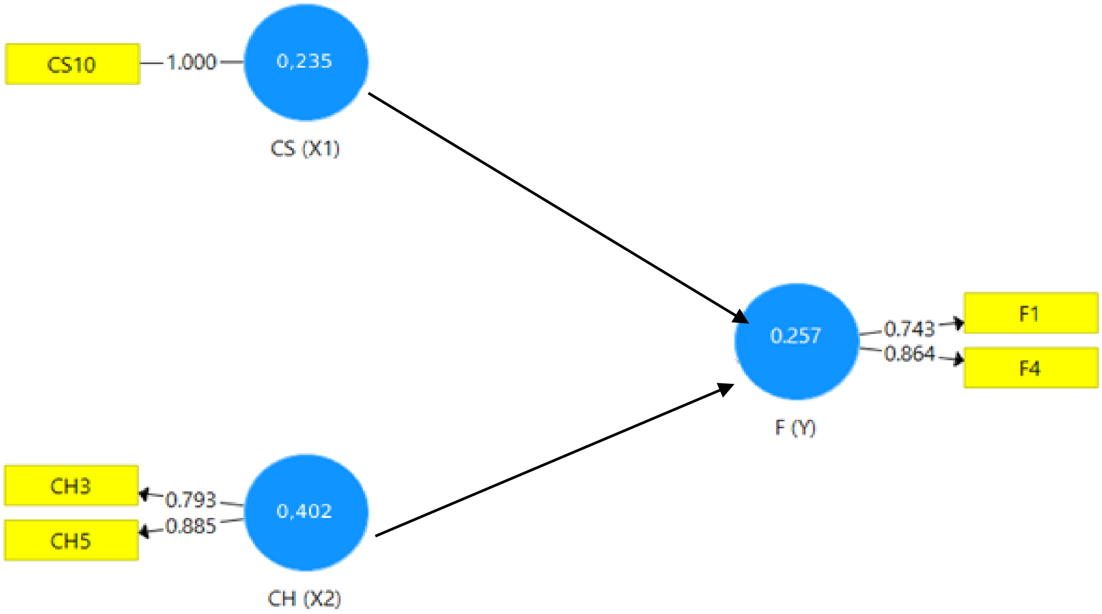

Figure 4. Measurement model / outside model.

The measurement model on the convergent validity of the reflexive indicators is assessed based on the relationship between the item score / component score and the construct score calculated by PLS. For individual reflexive measures, it can be said to be high if it is correlated > 0.70 with the construct to be measured. However, for research in the early stages of developing a measurement scale, a loading factor value of 0.50 – 0.60 is considered sufficient.

Table 1 presentation charging factor.

Table 1. Loading factor.

	CH(X2)	CS(X1)	F(Y)
CH3	0.793		
CH5	0.885		
CS10		1.000	
F1			0.743
F4			0.864

This study has a loading factor value > 0.70 so it can be declared valid. The first indicator on professional ethics there are 2 indicators, namely CH3 showing results of 0.793, CH5 of 0.885. The second indicator on independence has 1 indicator, namely CS10 with a result of 1,000. The third indicator has 2 indicators, namely F1 of 0.743, F4 of 0.864.

Table 2 presentation average variance extracted.

Table 2. Average variance extracted.

	Cronbach's	rho_A	Composite	Average Va
CH (X2)	0.589	0.617	0.827	0.706
CS (X1)	1.000	1.000	1.000	1.000
F (Y)	0.468	0.491	0.786	0.649

The Average Variance Extracted (AVE) variable for cyber security, cyber hardware, information systems against fraud > 0.50 which means that each variable has good discriminant validity. In discrimiant validity testing, the commonly used approach is the Fornell-Larcker Criterion (FLC) and Cross Loadings, which are indicators of latent constructs that are expected to be greater than the values of cross loadings on other latent constructs.

Table 3 presentation Fornell-Larcker criterion (FLC.)

Table 3. Fornell-Larcker criterion (FLC.)

	CH (X2)	CS(X1)	CS(X1)	F (Y)
CH (X2)	0.840			
CS (X1)	0.212	1.000	1.000	
F (Y)	0.452	0.320	0.320	0.806

The Fornell-Larcker Criterion (FLC) value in the CS variable has the highest FLC value in the latent construct itself, which is 1,000 compared to the FLC value in other constructs of 0.840, 0.806. The highest FLC latent construct value in the CH variable is 0.840. Variable F has the highest FLC value in its latent construct of 0.806.

Table 4 presentation cross loading.

Table 4. Cross loading.

	CH(X2)	CS(X1)	F(Y)
CH3	0.793	0.131	0.325
CH5	0.885	0.217	0.425
CS10	0.212	1.000	0.320
F1	0.354	0.143	0.743
F4	0.377	0.349	0.864

Based on the Table 4, it shows that the value of the relationship between the variable and its indicators is higher than the value of the relationship with other variables. Therefore, all latent variables have good discriminant validity or indicators in the indicator block of these variables are better than indicators in other blocks.

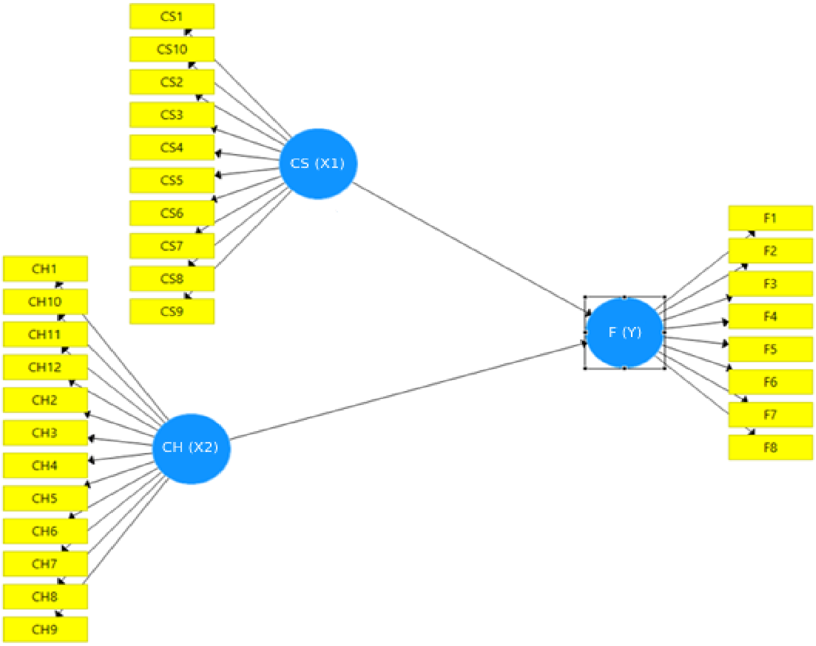

Figure 5. Structural model / inner model.

Figure 5 Illustration structural model / inner model.

Structural model testing aims to see the R-Square value for each endogenous latent variable to be the predictive power of the structural model.

Table 5 presentation Reliability test results.

Table 5. Reliability test results.

Variable	Crobach"s Alpha	Nilai	Keterangan
Cyber Security	0.80	0.700	Reliabel
Cyber Hardware	0.79	0.700	Reliabel
Fraud	0.75	0.700	Reliabel

The results of Cronbach's alpha reliability of cyber security instruments is 0.80, cyber hardware is 0.79, and fraud is 0.75. Of the three instruments that have Cronbach's alpha value > 0.7, namely cyber security and cyber hardware which are declared reliable or meet the requirements.

Table 6 presentation path coefficient.

Table 6. Path coefficient.

	CH (X2)	CS (X1)	F (Y)
CH (X2)			0.402
CS (X1)			0.235
F (Y)			

Cyber Security variable (X1) on Information System and Fraud variable (Y) has a path coefficient value of 0.235, which means that Cyber Security has a positive influence on Information Systems and Fraud. The Cyber Hardware variable (X2) has a path coefficient value of 0.402 on the auditor's performance variable (Y), which means that the auditor's experience has a positive influence on information systems and fraud.

Table 7. Reliability test results.

	Cronbach's	rho_A	Composite	Average Va
CH (X2)	1.000	1.000	1.000	1.000
CS (X1)	0.589	0.617	0.827	1.000
F (Y)	0.468	0.491	0.86	0.649

Based on the Table 7, it shows that the value of Composite Reliability (CR) on each variable is above 0.70. The cyber security variable has a CR value of 1,000, cyber hardware has a CR value of 0.827, fraud has a CR value of 0.786. With the value generated in the test study *Composite Reliability*, all variables have good reliability and are in accordance with the specified minimum value limit.

Table 8. Cronbach alpha results.

	Cronbach's	rho_A	Composite	Average Va
CH (X2)	1.000	1.000	1.000	1.000
CS (X1)	0.589	0.617	0.827	1.000
F (Y)	0.468	0.491	0,86	0.649

Based on the Table 8, it shows the results of the study that the Cronbach Alpha . value(CA) for the cyber security variable, which has a CA value of 1,000 > 0.70, this variable has a high level of reliability. The cyber security variable has a CA value of 0.589 < 0.70, the fraud variable has a CA value of 0.468 < 0.70 so it can be interpreted that these three variables have a low level of reliability.

Table 9. T-Test – statistics / bootstrapping.

	Original Sa	Sample Me	Standard D	T Statistics
CH (X2)- >	0.402	0.421	0.076	5.314
CS (X1) -> F	0.235	0.230	0.084	2.796

Based on the Table 9, it can be seen that the cyber security variable (X1) has a P-Values value of 0.000, cyber hardware (X2) has a P-Values value of 0.05. It can be concluded that these two variables have an influence on fraud.

Table 10. Test of determination or R – square / R2.

	R square	R Square A
F (Y)	0.257	0.242

Based on the Table 10, it has obtained an R – Square (R2) value of 0.257 or (26%). This shows that the percentage of the fraud variable by 26% in other words, these variables can be influenced by cyber security, cyber hardware, information systems by 26% while the remaining 74% can be influenced by other variables not examined in this study. The value of Q - Square in this study is used to determine the goodness of the model, namely the increasing value of Q - Square, the more suitable the structural model with the data.

Table 11 presentation Construct cross validated redundancy Q – square.

Table 11. Construct cross validated redundancy Q – square.

	SSO	SSE	Q2 (=1 – SSE)
CH (X2)	200.000	200.000	
CS (X1)	100.000	100.000	
F (Y)	200.000	172.874	0.136

The value of Q – Square on the endogenous variable is 0.136, which means that the amount of data diversity described in this research model is 13%. While the remaining 87% percentage is explained by other variables outside the research model. Therefore, this research model is declared to have met the requirements of goodness (model fit).

Table 12 presentation speculation results.

Table 12. Hypothesis results.

Hypothesis	T. Statistik	P. Value	Estimate	Hasil
H1	C3 – F	2.75	0.005	Diterima
H2	CH - F	5.31	0.001	Diterima

4.2. Discussion of Hypothesis Testing Results

The results of data processing carried out to answer the results of the proposed hypothesis, it can be seen that there are two acceptable hypotheses. This shows that there is a significant effect between the independent and dependent variables.

4.2.1. Effect of Cyber Security on Fraud

Based on the results of hypothesis testing, it is known that the T - Statistics value is 2.796 and the P - Values that form the influence of cyber security on auditor performance is 0.005 < 0.05, so it can be stated that cyber security has an effect on fraud. This shows that cyber security can prevent fraud. This happens because cyber security is able to ward off all kinds of crimes that come from hackers.

4.2.2. Effect of Cyber Hardware on Fraud

Based on the results of hypothesis testing, it is known that the T - Statistics value is 5.314 and the P - Values that form the effect of auditor experience on auditor performance is 0.000 < 0.05, so it can be stated that cyber hardware has an effect on fraud. This shows that cyber hardware can prevent fraud. This happens because cyber hardware is able to back up all kinds of viruses that enter the hardware.

5. Conclusion

Based on data analysis and discussion results, it can be concluded that Based on the hypothesis testing Test – T Statistics (Bootstrapping) that cyber security affect fraud, cyber hardware has an effect on fraud. Based on the value of R - Square (R2) of 0.257 or (26%). This shows that the percentage of the fraud variable by 26% in other words, these variables can be influenced by cyber security, cyber hardware, information systems by 26% while the remaining 74% can be influenced by other variables not examined in this study.

References

Anggono, A., & Riskiyadi, M. (2021). Cybercrime and cybersecurity in fntech: A systematic literature review. *Journal of Management and Organization, 12*(3), 239-251.

Aravazhi, M. S. (2020). Understanding cyber crime and cyber laundering: Threat and solution. *EPRA International Journal of Research and Development, 5*(1), 34-38.

Choi, K.-S., & Lee, C. S. (2018). The present and future of cybercrime, cyberterrorism, and cybersecurity. *International Journal of Cybersecurity Intelligence & Cybercrime, 1*(1), 1-4.Available at: https://doi.org/10.52306/01010218yxgw4012.

Das, S. R. (2019). The future of fintech. *Financial Management, 48*(4), 981-1007.

Fahlevi, M., Saparudin, M., Maemunah, S., & Irma, D. (2019). Digital cybercrime business in Indonesia. *E3S Web of Conferences*, *125*, 21001.Available at: https://doi.org/10.1051/e3sconf/201912521001.

Falco, G. (2019). Cybersecurity principles for space systems. *Journal of Aerospace Information Systems*, *16*(2), 61-70.Available at: https://doi.org/10.2514/1.i010693.

Gani, A. (2014). Cybercrime (Computer Based Crime). *Suryadarma University Journal of Information Systems*, *5*(1), 16–29.Available at: https://doi.org/10.35968/jsi.v5i1.18.

Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martinez-Caro, E., & Chinnaswamy, A. (2022). Resilience in healthcare systems: Cyber security and digital transformation. *Technovation*, *18*(1), 102583.

Hamed, A., Sobhy, A., & Nassar, H. (2021). Distributed approach for computing rough set approximations of big incomplete information systems. *Information Sciences*, *547*, 427–449.Available at: https://doi.org/10.1016/j.ins.2020.08.049.

Hawamleh, A. M. A., Alorfi, A. S. M., Al-Gasawneh, J. A., & Al-Rawashdeh, G. (2020). Cyber security and ethical hacking: The importance of protecting user data. *Solid State Technology*, *63*(5), 7894-7899.

Hayati, N. (2021). Social media and online gender-based violence during the covid-19 pandemic. *Journal of Law, Humanities, Society, and Culture (HUMAYA)*, *1*(1), 43-52.

Hilal, W., Gadsden, S., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. *Expert Systems with Applications*, *22*(31), 116429.

Jain, A., & Gupta, N. (2020). Cyber crime. *National Journal of Cyber Security Law*, *2*(2), 152-158.

Kaur, J., & Ramkumar, K. (2021). The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences*.Available at: https://doi.org/10.1016/j.jksuci.2021.01.018.

Lana, A. (2021). The impact of cybercrime on information technology and internal control. *Journal of Economics, Social and Education*, *1*(3), 1-13.

Mao, X., Sun, H., Zhu, X., & Li, J. (2022). Financial fraud detection using the related-party transaction knowledge graph. *Procedia Computer Science*, *199*, 733-740.Available at: https://doi.org/10.1016/j.procs.2022.01.091.

Paterson, T. (2019). Indonesian cyberspace expansion: A double-edged sword. *Journal of Cyber Policy*, *4*(2), 216-234.

Peters, G., Shevchenko, P. V., & Cohen, R. (2018). Understanding cyber-risk and cyber-insurance. In Fintech: Growth and Deregulation (pp. 303-330): Risk Books.

Sadino, & Dewi, L. (2016). Internet crime in electronic commerce. *Journal of Masters in Legal Studies*, *1*(2), 9–17.

Security, C. (2014). Criminology in the policy area of cyber security. *Scientific Journal of Aerospace Law*, *9*(2), 24–46.Available at: https://doi.org/10.35968/jh.v9i2.353.

Sulisrudatin, N. (2014). Analysis of cybercrime cases in the banking sector in the form of credit card data theft mode. *Scientific Journal of Aerospace Law*, *9*(1), 26–39.Available at: https://doi.org/10.35968/jh.v9i1.296.

Thaifur, A. Y. B. R., Maidin, M. A., Sidin, A. I., & Razak, A. (2021). How to detect healthcare fraud?"A systematic review". *Gaceta Sanitaria*, *35*, S441-S449.Available at: https://doi.org/10.1016/j.gaceta.2021.07.022.

Wall, D. S. (2008). Cybercrime: Digital Cops in a Networked Environment. Jack M. Balkin, James Grimmelmann, Eddan Katz, Nimrod Kozlovski, Shlomit Wagman, and Tal Zarsky (Eds.) (pp. 276). New York: New York University Press, 2006.

Wang, Z., Qi, D., Mei, J., Li, Z., Wan, K., & Zhang, J. (2021). Real-time controller hardware-in-the-loop co-simulation testbed for cooperative control strategy for cyber-physical power system. *Global Energy Interconnection*, *4*(2), 214-224.Available at: https://doi.org/10.1016/j.gloei.2021.05.004.

Zhang, Y., & Malacaria, P. (2021). Bayesian stackelberg games for cyber-security decision support. *Decision Support Systems*, *148*, 113599.Available at: https://doi.org/10.1016/j.dss.2021.113599.

Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2021). Dynamic defenses in cyber security: Techniques, methods and challenges. *Digital Communications and Networks*.Available at: https://doi.org/10.1016/j.dcan.2021.07.006.