Bulletin of Electrical Engineering and Informatics
Vol. 10, No. 3, June 2021, pp. 1658~1668
ISSN: 2302-9285, DOI: 10.11591/eei.v10i3.3028

Cyber-criminology defense in pervasive environment: A study of cybercrimes in Malaysia

Manmeet Mahinderjit Singh[1], Richard Frank[2], Wan Mohd Nazmee Wan Zainon[3]
[1,3]School of Computer Sciences, Universiti Sains Malaysia (USM), Penang, Malaysia
[2]Simon Fraser University, 8888 University Dr, Burnaby, BC V5A 1S6, Canada

Article Info

Article history:

Received Jan 29, 2020
Revised Nov 6, 2020
Accepted Apr 30, 2021

Keywords:

Cognitive hacking
Covid-19
Disinformation
MyCERT
Systemic approach

ABSTRACT

The growth of technologies; infrastructures and platforms with less or no security protection in emerging big data and internet of things (IoT) trends increase the likelihood of cybercrime attacks. With the rise of coronavirus disease-2019 (Covid-19) pandemic towards mankind, more cybercrimes are designed to penetrate one's cognitive mind in revealing sensitive details. In this paper; an exploration of cybercrime threats in Southeast Asia country; Malaysia from year 2008 up to 2020 and its hike trends and impacts will be discussed. An investigation revolving the study of cyber-criminology and the reasoning behind the growth in terms of technological advancement will be presented. The findings suggest that the consequences and impacts of the cyberspace attacks are beyond the loss of money and reputations. It now becomes the failure of the global systemic altogether. As a mechanism to handle this would be to focus on protecting mission critical applications in pervasive environment. In this paper, a comprehensive authentication and authorization framework in safeguarding applications and users in the pervasive environment will be presented.

Corresponding Author:

Manmeet Mahinderjit Singh
School of Computer Sciences
Universiti Sains Malaysia, Penang Malaysia
Email: manmeet@usm.my

1. INTRODUCTION

The advancement of big data and internet of things (IoT) technology trends in the gathering; processing and generating intelligence services have impacted our life towards betterment. The high-volume data gathered means more valuable information generated in terms of analytics, which could act as predictive and prescriptive in various domains such as health care; e-commerce; transportation and others. The increased cybercrime due to Covid-19 in 2020 worldwide are at its perilous magnitude causing losses in terms of money and trust towards technology [1] mentioned above. The study of cyber-criminology integrates both the domain of criminology sociology and psychology but towards crimes leveraging the cyberspaces specifically. The definition of cybercrime revolves around the offence or crime committed in cyberspace through tools such as a computer; smartphones using a network system intending to breach confidentiality, integrity, and availability [2] of any assets. There are many purposes of cybercrime act which include financial gain, entertainment, and activist for political or religious purpose and for revenge [3]. The impact of any security attacks may lead to losses in monetary, reputation and even nation sovereignty [4].

One main catalyst of crime in cyberspace is due to its nature and characteristic which conform to dynamic spatial temporal coupled with identity flexibility, anonymity and lack of deterrence [5]. The nonexistence or blurs the line between space and time in cybercrime and traditional based crime leads to

online offenders getting away from being tracked. The usage of technology such as a smartphone is booming in ASIA Pacific [6]. China, South Korea, and Malaysia recorded more than 50% of it are the country's populations as mobile device users [6]. Accordingly, Petrenco (2019) [7] claimed cyber-attacks as the 6th most impactful global risk. Another study shows that overall internet scam victim faces a loss of more than USD 400 million globally [8].

The challenges with tackling cybercrime worldwide lie in the failure to dully understand the systemic relationship within cybercrime stakeholder's relationship and the sociology impact of criminology towards cybercrime. With lesser study of cyber-criminology which integrates criminology field to cybercrime; most of guardianship system are not designed properly. Systemic failures in understanding human behavior, environment effect studied in criminology theories and the mapping between this sociology theories with cybercrime are still in its infancy. For instances, according to routine activity theory [9], [10]; comprehensively presented the criminology actors which is attacker, victim and guardianship in any criminology equation. The theory might be relevant as well to cybercrime context. Even the crimes are conducted using technology and Internet infrastructure, an attacker and victim are viable. The guardianship here is transformed from policing to system related preventions and detections system. There are many other criminology theories such which could clearly be mapped to cybercrime which are still not fully understood [11], [12]. Thus, in this paper, an exploration of criminology theories and cybercrime is presented. The main objective of this paper is to focus on Malaysia for further discussion on the kind of cybercrime attacks occurrences in Asian Pacific. An analysis obtained via MYCERT from 2008 to 2020 will be analyzed and the reasoning behind the time series trends will be presented. An approach to mitigate the attacks by employing the first line of defenses utilizing Identification and authorization framework is presented. The outline of the paper is as the following. Section 2 presents an overview of Cybercrime and the efforts conducted in the Asia Pacific to tackle this crime. Section 3 presents the analysis done based on the secondary data observed from Malaysian computer emergency response team (MYCERT) for a span of 12 years (2008-2020). The justifications and in-depth analysis are presented as well. Finally, a section on significant analysis, authentication framework and conclusion is stated as well.

2. CYBER-CRIMNIOLOGY ANALYSIS

The mapping between the field of criminology and cybercrime known as cyber-criminology is not easily quantified and understood. The difficulties of clearly distinguishing traditional crime and cybercrime are closely related to how crime occurs and the factors that cause the crime [13]. Table 1 demonstrates some well-known cyber-criminology analysis. The link between cybercrime and security attacks is shown by classifying three stakeholders which are the offenders, the victim, and the guardianship.

Many theories mapped demonstrates the offender's perspective. This means; by carefully perceiving offenders' behaviour in physical space; similar behaviour is transformed towards criminal activity in cyberspace. Modelling these traits and quantifying these traits and studying the relationship between physical device usage and behaviour could present a new guideline in thwarting cybercrime. In the next section, a brief discussion on Identity threat and mobile computing threat will be presented.

2.1. Cyber-criminology relationship for identity theft threat

According to Javelin and Strategy [9]; in 2017; 15.4 million consumers were the victim of Identity theft in which $16 billion loss was reported worldwide. This makes identity theft a very lucrative illegal business. Normally; Identity theft threat leads to transaction-based crime such as credit card fraud; bank account compromise; PayPal account compromise and social media account impersonation which leads to love scams. Users' personal information such as name; identification ids, address or even account numbers could be used for these purposes. With the advancement and anonymity provided by TOR browser; marketplaces such as dream market and sell identity theft related information in the form of credit card or documents such as passport. Figure 1 shows some products sold in the Dream Market collected via Darknet. There are many method cybercriminals used to obtain credit card details. Among them are as the following:

- Stolen/theft card: Any stolen credit card is the easiest form of attack in which financial data obtained is then sold on the Darknet platform for less than USD 50. Some online transactions only require your credit card number, CVV number and expiry date.
- Phishing attack: An attack either done through web defacement, emails or through phone calls. The modus operandi here is to receive a call from authority canters such as commercial banks or tax department requesting some verification on bank details. Once obtained; details will then be sold elsewhere.
- Application based attack: This is the latest threat known as form jacking. Consumers normally visit an infected online retailer without using a comprehensive security solution, leaving their valuable personal

and financial information vulnerable to potentially devastating identity theft. According to Symantec [10]; form jacking has become a lucrative choice cyber crooks, though it's impossible to quantify the amount stolen from every form jacking attack in 2018.

- Skimming device: Duplicate devices are placed on ATM in which this device will record all the transactions made. The recorded details are then transferred to a computer in which the details are then sold to others.
- Account takeover: This attack takes place when the detail of the credit card is obtained during hand first. Next, the attacker would call in the banks and change the billing address.

Based on the mapping of cyber-criminology; two main theories such as general theory and neutralization theory can be applied to the trait and behaviour of offenders. With lack of deterrence tools to catch the offender and blur law in prosecution; no wonder identity theft becomes a lucrative crime. Next; mobile computing threat is discussed.

Table 1. Cyber-criminology analysis

Criminology Theory	Cybercrime Stakeholders	Criminology Theories Concepts	Cyber-criminology Mapping	Security Attacks
Anomie Strain theory [14]	Offenders	Innovation leads to crime in which offender use innovative means yet illegal to achieve wealth	Offenders adopt innovative approaches in cyberspace using existing tools in penetrating networks and system to gain financial gain	Organized Crime Hacking
Routine Activity Theory [15]	Offender-Victims	Crime occurs when three elements converge: (1) a motivated offender, (2) a suitable target, and (3) the absence of a capable guardian	Similary, to cybercrime stakeholders; any cybercrime event occurs when three elements converge: i) attacker, ii) victims and iii) defender	Any cyberattacks
Rational Choice Theory [16]	Offenders	Cost -benefit of crime, the likelihood of detection and severity of the punishment	Decision making in any cybercrime involves evaluating cost-benefit and even the likekuhood of being detected or tracked	Hacking
Differential Association Theory [17]	Offenders	Criminal behavior learned in a process involving interaction and communication with others	Cybercriminal tend to share knowledge, tips and create forums to interact electronically and share an interest	Hacktivist Subculture Digital Privacy Cyberterrorism
General Theory of Crime [18]	Offenders	A mount of (lack of) control placed by law; society scholl; family differentiates criminal to non-criminal	Most crimes provide immediate gratification with minimal thought over consequences of actions.	Online harassement; Economic crimes; Identity theft and Hacking
Moral Development Theory [19]	Offenders	Criminal behavior arises when an opportunity to offend occurs and there is a delay in the development of moral reasoning in the individual	There have been many documented anecdotal accounts of the lack of concern by hackers over the systems they have attacked	Any cyberattacks
Social Learning Theory [20]	Offenders	Criminal behavior is acquired through observational learning	Cybercriminal conduct crime by imitation and modelling from others	Hacking
Cultural Lag [21]	Guardianship	Failure to dvelop social consensus on the appropriate application of modern technology leads to a breakdown in social stings.	Any application/technology designed with no regard of protection lead to a human being the weakest link	Any cybercrime
Digital Drift Theory [22]	Offenders	Internet interactions which require no face-to-face and borderless could drift non-criminal towards criminality	Some offenders get drifted into becoming cybercriminals due to internet pseudoreciprocal environment	Child pornography/Online harassment
Space Transition Theory [5]	Offenders	Explanation about the nature of the behavior of the persons who bring out their conforming and non-conforming behavior in the physical space and cyberspace.	Factors such as offenders behavior; the social settings they live in and the internet features lead to cybercrime.	Any cybercrime
Situational Crime Prevention [23], [24]	Guardianship	Crime can be reduced by altering situations rather than an offender disposition.	Implementation of the defender/guardianship system reduces the likelihood of crime	Any cybercrime

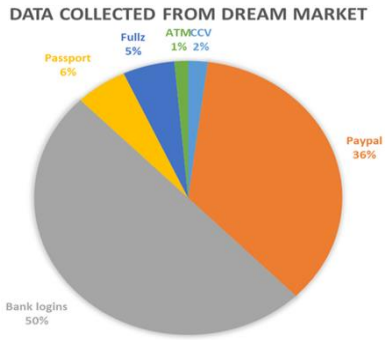


Figure 1. Identity theft data sold in dream market in 2019

2.2. Exploration of cyber-criminology efforts in ASEAN countries

With the use of cyberspace; there are zero spatial distances. This becomes non-trivial, especially when prosecuting crimes and crimes that occur between different countries and jurisdictions laws. In order to deal with these transnational crimes; The council of Europe in 2001 has introduced a convention on cybercrime known as the budapest convention to allow collaboration among states for transnational cybercrime investigation and prosecution. Not all countries ratified this convention. For instance; The association of Southeast-Asia nations (ASEAN) country consisting of Singapore, Indonesia, Malaysia, Philippines, Thailand, Vietnam, Laos and Myanmar did not ratify this convention. ASEAN, which was established in 1976 [25] to promote peace and cooperation only did recognize. Cybercrime as a transnational crime during the 2004 Joint Communique of the fourth ASEAN ministerial meeting [26]. Thus; the outcome of the meeting leads to strategic planning in term of legalization and jurisdictions between ASEAN countries. In order to enforce a platform of collaborations and sharing of cybercrime events; ASEAN telecommunications and IT ministers (TELMIN) established national computer emergency response teams (CERTs) in 2003 [27]. Other two initiatives which focus is providing awareness to the public; to impose sustainable partnership between private and public sectors and discuss issues relating to cyber terrorism and cybercrime are ASEAN ICT masterplan 2015 (AIM 2015) [28] and ASEAN regional forum (ARF) [29].

2.3. A study of cybercrime enforcement and laws in Malaysia

In Malaysia, the computer crimes act 1997 is used to combat cybercrime attacks [29], [30]. However, this law only covers the misuse of computers and does not cover does not cover many areas of computer-related activities. Digital Signature Act 1997 [30], [31] provides measurements to secure online transaction by using digital signature and copyright act 1997 [30], [31] protects against infringement of copyrights. In order to regulate and e-commerce transactions and processing of personal data; act such as the electronic commerce act 2006 [30], [31] and personal data protection bill 2010 [30], [31] are used. Few government institutions are responsible for handling cyber threat issues such as the ministry of science, technology, and innovation (MOSTI) and the Malaysian communications and multimedia commissions (MCMCs) [32]. MOSTI is responsible for designing a framework regarding the national policy of ICT. It aims to design policies to secure the critical national information infrastructure (CNII). CNII is integrated with every asset, whether physical or virtual, system and function, that is important to the nation and its security is essential [33] [34]. In order to deliver technicality security services and protect NCSP policies; Cyber security Malaysia (CSM) was created. CSM is responsible to run services relating to emergency services; quality management; professional development and strategic engagement and research [32]. In addition, MOSTI also supervises the computer emergency incident known as Malaysia computer emergency respond team (MyCERT) [35]. MCMC on the other hand; regulates communication and multimedia activities covering broadcast, internet service provider (ISP), postal and courier, and authority of digital certificate [32]. Next; some insight on cybercrime attacks in Malaysia and its justifications will be shared.

3. RESEARCH IN-DEPTH ANALYSIS: CYBER CRIME CASES IN MALAYSIA

Based on computer emergency response teams (CERTs), a platform to coordinate computer incident information reporting and sharing; reported cybercrime attacks in Malaysia since 2008 to 2020 has been analyzed. Prior to the cybercrime attacks being discussed; the notion of what consist within the cybercrime categories will be discussed. Table 2 displays the categories of incidents and its subcategories.

Among the categories are; i) privacy breaches; ii) transaction based attack; iii) alteration of data; and iv) disruption of normal operations. Privacy breach involves an attack leading to sensitive information

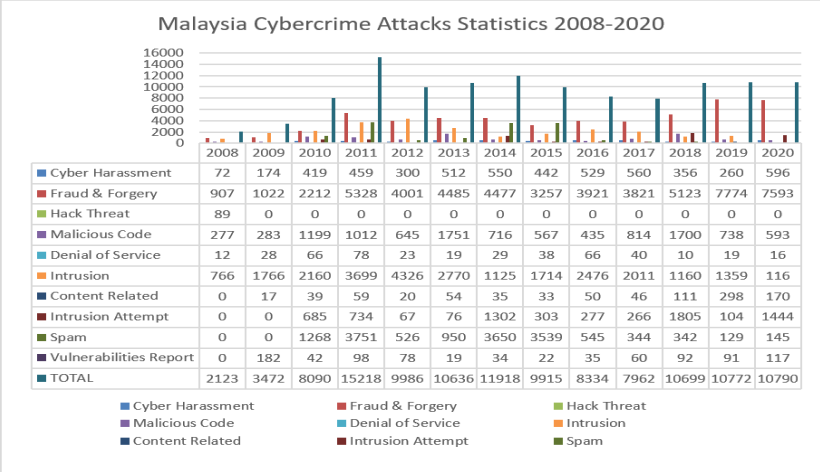
leakage such as intrusion attacks (account compromise; defacement) and spamming (spam relay; email spam). Malicious code category consists of botnet control and command (C&C) and malware threats which could lead to information leakage, alteration and destruction. The impact leads to a loss in data integrity and decreases of trustworthiness. Another category which causes disruption of normal behavior is through denial of service (DOS) which is launched by bots. The effect here is unavailability of services; system or network. Finally; transaction-based crime is the fourth category. Attacks such as fraud and carding impact the economy in term of loss of money and lead to a loss in term of confidentiality, availability and integrity of data and systems.

Table 2. Categories of incidents and its subcategories

Categories of Incidents	Subcategories
Cyber Harassment	Cyberbullying, Cyberstalking, Sexual, Religious, Racial
	Phishing, Fraud Transaction, Online Scam, Counterfeit Items
Fraud & Forgery	Unauthorized Transaction, Illegal Investment, Nigerian & Online Scam
Malicious Code	Bots, C&C Botnets, Malware, Malware Hostings
Denial of Service (DOS)	Denial of Services (DOS)
Intrusion	Account Compromise, Defacement
Content Related	Pornography, Intellectual Properties, National Threat (Disinformation (Fake News)
Intrusion Attempt	Port Scanning, Login Brute Force, Vulnerabilities Probes
Spam	Spam, Spam Relay
Vulnerabilities, Report	Misconfiguration (Disclosure), Web, System

3.1. Distribution of Malaysia cyber crime attacks from 2008 to 2020

The data analysed from 2008 up to 2020 is generated from the source of incidents reported either by home users or business owners. Figure 2 demonstrates the analysis of this data presented based on reported cases yearly. Overall, there were 109034 incidents recorded within this of time. This more than 100 k incidents recorded is at its minimal and determines that there are still many cases which are not reported. Next, the analysis of the cases reported will be discussed. This analysis would include justifying the intense growth of attacks by observing factors such as growth and emerging of technological and cybercrime attacks from 2008 to 2020.



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Cyber Harassment	72	174	419	459	300	512	550	442	529	560	356	260	596
Fraud & Forgery	907	1022	2212	5328	4001	4485	4477	3257	3921	3821	5123	7774	7593
Hack Threat	89	0	0	0	0	0	0	0	0	0	0	0	0
Malicious Code	277	283	1199	1012	645	1751	716	567	435	814	1700	738	593
Denial of Service	12	28	66	78	23	19	29	38	66	40	10	19	16
Intrusion	766	1766	2160	3699	4326	2770	1125	1714	2476	2011	1160	1359	116
Content Related	0	17	39	59	20	54	35	33	50	46	111	298	170
Intrusion Attempt	0	0	685	734	67	76	1302	303	277	266	1805	104	1444
Spam	0	0	1268	3751	526	950	3650	3539	545	344	342	129	145
Vulnerabilities Report	0	182	42	98	78	19	34	22	35	60	92	91	117
TOTAL	2123	3472	8090	15218	9986	10636	11918	9915	8334	7962	10699	10772	10790

Figure 2. Incident statistics for cybercrime attacks from 2008 to 2020

3.2. Analysis and justifications of cybercrime attacks from 2008 to 2020

The analysis conducted will be based on several key constructs as the following:

a. 2008: 2010: The stead and linear hike of attacks

Data recorded from 2008 to 2010 display a linear and steady hike of cybercrime attacks four types of attacks. There are also two new attacks reported in 2010 which are spamming and intrusion attempt. Two attack types; Fraud & forgery (F&F) and Intrusion display a trending increase with the highest recorded cases in 2010 with F&F (2212) and Intrusion (2160). Both attacks categories contribute almost 55% of the overall reported cases in 2010. Fraud and forgery (F&F) attack category involved cases such as phishing; fraud transaction via e-commerce sites; online scam; unauthorized transaction; and counterfeit items. Meanwhile,

intrusion involves cases such as web defacement and account compromise [33]. Both attacks are interrelated to malware threats. There is also a cause-and-effect relationship between these attacks. For instance, phishing emails always lead to victim accessing the defaced website and fraud transaction such as credit cards involve account compromise attacks to occur.

b. An outlier recorded in 2011 attacks.

Based on Figure 3, 2011 shows an usual outlier of reported cases. There has been an increase of 88% of cases numbers compared to previous years. Three main attacks dominating the charts are the F&F attacks: Intrusions and spamming attack. The shifting growth of technology is among the factors for justifying this report. Right before 2008; the innovation of supercomputers and nanotechnology in powerful chip design; power-saving batteries and emerging technology of mobile computing have already taken place [36]. However; it's only in the year 2008 to the end of 2009; technologist companies began to improvise their business model with more added functionality service into this innovation. Interesting; as stated in the Telegraph UK [37]; 2008 and 2009 also demonstrates a widespread of apps markets like Google plaster and Apple Store; the development of satellite navigation with the adoption of GPS in mobile phones and new phones such as Microsoft Phones and social messaging's account growth (Facebook and Twitter). By the end of 2010; 3D technology innovation; added location-based check-ins services and the Android based Smartphone were well accepted by the consumer [38]. With Facebook is recording a staggering 500 million users across and adoption of mobile computing everywhere; the outbreak of trends and technologies has also influenced the growth of cybercrime attack. This is proven when in 2011; an increased in hacktivism occur. Hacktivism is an improvised term of hacking in which the motivations of penetrating into a system are beyond personal fun or gain. Hacktivism tends to attack the system to change the social setting; thus, changing political and business agenda and prospecting in which cases of hackers accessing personal user data. One main reason contributes greatly to increases of malicious code; intrusion and even spamming is the fully functional open network such as Android Play store [39]. The issue with the open platform such as Android; application requires no code signing. The vulnerabilities that exist within these services is severe with anyone can upload and download an app regardless of its authenticity. With the advancement in hacking and maturity of smartphones and other mobile based products; 2011 display a hike in term of incidents recorded. Spam; an attack in which involves sending unsolicited advertising, too many recipients be used to deliver Trojan horses, viruses, worms, spyware, and targeted phishing attacks. Thus, spamming act becomes the agent for both fraud such as phishing and intrusion such as account compromise and defacement to take place. The high cases of intrusion such as account compromise and web page defacement are probably due to events such as LinkedIn account compromises that occur in 2012. Cyber-attacks launched into social media platforms and websites used by millions would ensure impact the users in Malaysia.

c. 2008 to 2011: Trending increment of cyber harassment & malicious code

Based on the incidents recorded; cases of cyber harassment and malicious code shows a constant increment from 2008 up-to 2017. Increase the level of cyber harassment such as cyberbullying highly contributes to the nature of the Internet which is anonymous and the adoption of social messaging such as Facebook among youth. With the benefit of anonymity and pseudonyms, cyber bullying cases recorded a drastic increment.

d. 2011 to 2019: An analysis on comparisons of recorded cases

An analysis of categories of an incident from 2011 to 2019 as shown in Table 3 is to display the overall total cases based on categories and the comparison of an incident from 2011 to 2019. The highest numbers of recorded incidents are fraud incidents which display 47328 cases. Second highest would be Intrusion with 25332 cases and third and fourth placing followed by Spam (15044) and Malicious code (10137). Fraud and forgery involve attacks such as phishing, fraud transaction, unauthorized transaction, and Nigerian love scam. Fraud remains to show increment in terms of attacks reported.

Based on the comparison of attack incidents recorded, there seem to be some interesting findings. Overall; there has been a reduced number of cyber harassments; DOS: Intrusion and spamming attack recorded. The reasons could be awareness among Malaysia users, which could have been heightened, especially for attacks such as spamming. Besides, another phenomenon is where the crime is not reported by a victim of cyberbullying and cyberstalking. The numbers of incidents from the categories of content related attacks; malicious codes and intrusion attempt shows a reduction int terms of threat percentage differences between 2011 and 2019. Malicious codes (-27%), intrusion attempt (-63%) are malware-based threats. A new threat classification involving content related shows a high increment from year 2011. This is the latest threat in which content such as pornography; IP infringement and national threat with cases of disinformation (fake news) are nowadays recorded. As Malaysia; a multiracial country; the increased on the national threat is worrying, especially when social media is used to spread disinformation events such as fake news and events. Nevertheless, even though the comparison between 2011 and 2019 shows a slight reduction in fraud; overall records showing the high numbers of fraud cases demonstrate the impact and severity of this attack.

Table 3. Comparison of total incidents and its trending percentage from 2011-2019

Categories of Incidents	2011	2019	Total Incidents	Percentage (%)
Cyber Harassment	459	260	4633	-43%
Fraud & Forgery	5328	7774	46328	46%
Hack Threat	0	0	89	0%
Malicious Code	1012	738	10137	-27%
Denial of Service	78	19	428	-76%
Intrusion	3699	1359	25332	-63%
Content Related	59	298	762	405%
Intrusion Attempt	734	104	5619	-86%
Spam	3751	129	15044	-97%
Vulnerabilities Report	98	91	662	-7%
TOTAL	15218	10772	109034	-29%

e. New attack in 2018 onwards

One interesting analysis based on MYCERT reports [35] is several new cases of ransomware attacks reported in 2018. Almost 16 cases were reported either by home users: business owners or government services. Ransomware is a severe malicious attack in, which is designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. In 2019; ransomware is seen as a malware which, coupled cripple healthcare systems and governments. Ransomware attacks were a part of the 298 cases reported under the category of content related. Another attack under this category is the rise of disinformation cases reported such as fake news. Based on the analysis conducted and technological justification presented; it is clear the existence of the relationship between technology trends such as big data and IoT with growing numbers of cybercrime attacks. Cyber-criminology, a globally threat deserves attention and calls for mitigation strategies. However, the solutions here is not solely for the use of technological guardianship, such as cybersecurity solutions or enforcement of laws; jurisdiction and security bodies; but a larger systemic plan incorporating component such as technology trends developers; legal systems; consumer (individual) and society (diverse background of culture and ideology) to introduce international based policies and regulations. However, as mentioned by [17], [36]; any regulations and policies will only work when any government enforcements on the policies are observed and monitored. Another context is the emerge of attacks which manipulate cognitive ability such as ransomware, phishing and disinformation cases. Human incapability of making poor decision and blindly trusting are the main factors which lead towards the leap of these cases.

f. Covid-19 pandemic leading to cybercrime attacks due to cognition hacking.

Covid-19 pandemic has caused catastrophic impacts which affect the welfare of citizens, the economics of a country and most of all the social being of people. With countries locking down their border physically, the consumption of internet has spike worldwide. One innovation adopted by both public and private organizations and government agencies is "working from home" (WFH). The high usage of the internet during WFH also becomes an enabler to the global rise of cybersecurity threats globally. With more than 600% phishing attempt, recorded since February 2020, almost 1000% increase of the malicious websites with contents-themed coronavirus has been recorded [35]. According to the Malaysian Crime Prevention Foundation (MCPF), the total losses recorded regarding cybercrime for 2019 and 2020, were RM305 million and RM247 million, respectively. Based on the comparison of attack incidents recorded, there seem to be some interesting findings. Based on Table 4 analysis, an increased number of cyber harassments (129%); Intrusion attempts (1228%), spamming (12%) and vulnerabilities report (137%) attacks were recorded. Due to the high adaptation of WFH among public and private organisations and high-speed internet connections in urban area, cybercrime attacks could be launch easily. By adaptation of traditional attacks and threats techniques such as spear phishing or ransomware, Covid-19 keywords were embedded within emails contents or URL listings to capitalize on user's fear. Comparison between fraud & forgery cases between 2019 and 2020 show a little fraction of reductions which is around 181 cases (-2.3%). Although the number has reduced, the high numbers of fraud cases such as phishing cases during Covid-19 pandemic is alarming. Failures of organization in preparing a comprehensive business continuity and incident response plans in hand and lack of enforcement mechanisms are among factors of employees being convenient targets of cybercrime attacks. Lack of cybersecurity training and awareness campaigns by top managements prior to pandemic can be reflected on the high numbers of recorded attacks. Overall, even though there seem to be a slight attack recorded in contrast to 2019 (+0.18%), the impact cybersecurity due to Covid-19 in Malaysia would need to be tackled quickly. In 2020, cognitive hacking-based attacks will become more severe. Technology and trends adoption and acceptance by Malaysian contributes strongly towards the hikes as well. Lack of awareness and knowledge in securing technological based devices such as mobile computing devices

and its users are the culprit towards the cybercrime threats hike. Thus next, a model of authentication to ensure basic security hygiene in a pervasive environment will be proposed.

Table 4. Comparison of total incidents and its trending percentage from 2019-2020

Categories of Incidents	2019	2020	Total Incidents (2019-2020)	Percentage (%) of Attacks Increment & Decrement
Cyber Harassment	260	596	856	129%*
Fraud & Forgery	7774	7593	15367	-2.3%
Hack Threat	0	0	0	0%
Malicious Code	738	593	1331	-20%
Denial of Service	19	16	35	-16%
Intrusion	1359	116	1475	-91%
Content Related	298	170	468	-43%
Intrusion Attempt	104	1444	1548	1288%*
Spam	129	145	274	12%
Vulnerabilities Report	91	117	208	137%*
TOTAL	10772	10790	21562	0.18%

4. DISCUSSION: SAFEGUARDING CYBERSPACE WITH AUTHENTICATION & AUTHORIZATION

Authentication remains as the first defense in any mission critical applications such as IoT, mobile based applications and even for mission critical application which is apart of the fourth industrial revolution (4IR). Among the mechanisms involves adopting multifactor authentications integrated with strong hashing algorithms besides encrypting other essential information's. In practice and as shown in Figure 3, mission critical applications involve three main stakeholders which are the mobile users, applications and servers. The main essential in any authentication models is to comply with security by design model. Each pervasive application differs based on its functionality and its design and requirements. Similarly, each application and pervasive domain has different types of system vulnerabilities and threats. Next, for any mission critical applications and domain, the need to have authentication protection for identifying human to human, and device-to-human communications is essential. Finally, any metadata within the application should be protected based on its sensitivity. Each sensors data captured should be automatic annotated based on its sensitivity [40]. Sensors such as GPS which stands as a sensor that leads to leakage of one's locations information's has a high sensitivity in contrast to accelerometer sensor [40]. This information is then could be inputted as in designing access control in terms of adding user permission and its level. Another promising path is in the protection of metadata using technologies which are secure and tamper proof such as blockchain technologies [41]. The mechanisms of authentication are divided based on authenticator IDS, channel/communications, protocol and technologies and authentication requirements. Figure 3 display authentication and authorization model for safeguarding mission critical application in a pervasive environment. Next, we will present the four-authentication mechanism which are the authenticator ID, channel/communications, protocol and technologies and other identification requirements.

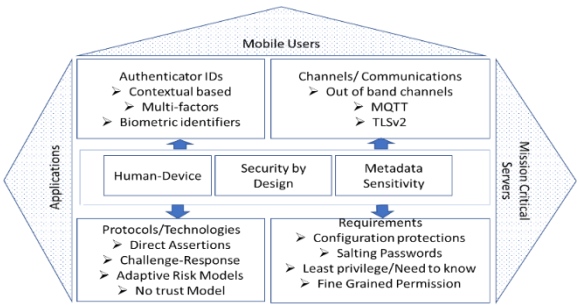


Figure 3. Authentication and authorization model safeguarding mission critical applications in pervasive environment

4.1. Authenticator IDs

The identifiers or features that become the input to identify a user has emerged beyond simple text-based passwords. With the latest technologies' advancement, the need to use biometric based identifiers are becoming acceptable and practical. This is because biometrics are unique and cannot be masqueraded. Biometrics identifiers adopted here could originate from hard (fingerprint, face) and soft (keystrokes, voice) identifiers. When a single biometric or unimodal biometric identifier is integrated with other factors such as

password, token or proximity sensors technologies (NFC, RFID), the outcome leads to a multi-factor-based system. Nevertheless, the factors mentioned are also capable to be merged with contextual factors (time, location, behavior and user ID) to support applications and systems based on the sentient environment [42]. Applications protected and accessible based on contextual information's are important to permit authorized user access during a certain time and limiting full access within the restricted perimeter.

4.2. Channel/communications

Most of the pervasive applications stored and used online are communicated through unprotected HTTP browser. The need to protect the communication between stakeholders such as mobile users accessing applications with the applications server need to be done using channels such as MQTT and SSL/TLSv2. Another promising method of authentication which is adopted in wearable technologies is by employing out of band channels. Here two different frequency bands such as WIFI used by Smartphone communicating with the broadband provider and Bluetooth channel used between smartphone and wearable device. In term of security, this kind of authentication is prone to inherit all the vulnerabilities of WIFI and Bluetooth. But the positive sides is the flexibility of adding security protection device such as a Smartphone to protect wearable devices.

4.3. Authentications protocol and technologies

In any mission critical based applications, the need to adopt an adaptive risk model has become major importance. The usage of one-time password (OTP) within system ensures timeliness and most of all thwarts against most of the security attacks such as phishing attack, password attack and even fraud revolving financial systems. Challenge-response is also a key in handling attacks of ecommerce transaction attacks. Another important protocol needs to be tapped into any applications is the direct assertions [43]. As most of the authorization permission is given right after the user authenticate themselves, this could lead to the issue of an unauthorized user still manage to brute force and penetrate a system. With most of the system defined to allow least privilege, this unauthorized and informed guest can at least read any files [44]. The correct way is for all authorization permissions and rights should be accessed for a user before this user is invited to authenticate himself [44]. The usage of direct assertion [43], [45] could be the answer to all the security issues revolving any technology and applications. Finally, with the importance of each device and users no trusting each other, the need for all connected devices and user to be accessed before the authentication process is essential.

4.4. Other authentication requirements

Other essential requirements for any applications when it comes to authentication would be to add features of protections in its configuration files. All pervasive applications have a configuration file in which metadata containing details such as mobile standard, types, its version, password of admin, IP address, etc are stored. Normally this configuration files could be accessible by the application users. In an event, if the configuration files are accessed by hackers, the leakage of metadata of the applications and even the devices could take place [46]. As one way of safeguarding configuration files is by using a shadow file mechanism. In this approach, the configuration files contain a pointer to another location which is accessible only by authorized administrators [47]. This second layer of defense in depth can be further integrated with strong password mechanism by using salting random numbers with user password [48]. With salt being used, the chances of password duplication and brute force of password are minimized. Another requirement is in driving access control system towards only allowing least privilege access and in accordance to need to know principles should be applied [49]. A user is only given access based on their needed tasks with the lowest clearance such as to read. This will also ensure that any permission on object or functionalities of an application is presented in a fine-grained manner [50]. Overall, the presented model is capable to secure and safeguards applications from both security and privacy attacks targeting mobile applications transaction online.

5. CONCLUSION

An analysis of cyber-criminology based on technological factor and temporal effect are presented in this paper. The comparison cyberattacks in Malaysia reported in MyCERT is analysed for span of 12 years since 2008 to 2020. With new type of cybercrime threats emerging such as ransomware, spear phishing and disinformation threats have a theoretical relationship with technology advancement and user's exposure towards this technology. Based on the analysis; findings demonstrate that there is a direct consequent between technology and cybercrime. Second findings show crime appearing on cyberspace has transformed from traditional crime. Based on criminology research; there is a clear transformative between stakeholders; the security attacks and criminology theories. With cyberspace technology, many applications are designed for pervasive environment. Most of mission critical domains such as financial; national security systems; military have its implementation of applications designed for mobility advantage. It is crucial to ensure these

mobile based applications are protected against any security vulnerability derived from the physical technology; weakness and exploitation from the software design and most of all the users who are novice. A framework on authentication and authorization for safeguarding any mission critical applications is presented at the end of this paper. In future, the framework will be extended into a working prototype and further testing on its usability will be done in depth. By referring to the phrase "a chain is only as strong as the weakest link", vulnerabilities and loopholes in technologies and cyberspace platform are here to stay. The fastest yet harder method for solution would be in educating technology users to protect their personal data and systems. This is only achievable when user claim accountability and control in their own technology usage and perceive that security is always an afterthought in any technology developed. In conclusion, cease of being the weakest link of the chain.

REFERENCES

[1] W. Kim, O. R. Jeong, C. Kim, and J. So, ''The dark side of the Internet: Attacks, costs and responses,'' *Information Systems*, vol. 36, no. 3, pp. 675-705, May 2011, doi: 10.1016/j.is.2010.11.003.

[2] J. M. Drew, ''A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies,'' *Journal of Criminological Research, Policy and Practice*, vol. 6, no. 1, pp. 17-33, 2020, doi: 10.1108/JCRPP-12-2019-0070.

[3] S. B. Harmandeep and G. Kumar, ''Cybercrimes: A Proposed Taxonomy and Challenges,'' *Journal of Computer Networks and Communications*, vol. 11, 2018, doi: 10.1155/2018/1798659.

[4] F. Malecki, ''Best practices for preventing and recovering from a ransomware attack,'' *Computer Fraud & Security*, vol. 2019, no. 3, pp. 8-10, 2019, doi: 10.1016/S1361-3723(19)30028-4.

[5] K. Jaishankar, ''Space Transition Theory of cyber crimes,'' *Crimes of the Internet*, Upper Saddle River, NJ: Prentice Hall, 2008, pp.283-301.

[6] A. L. Mutchler, J. P. Shim, and D. Osmond, ''Exploratory Study on Users' Behavior: Smartphone Usage,'' *AMCIS* 418-425, 2011.

[7] S. Petrenko, ''Cyber Resilience,'' River Publishers, 2020, pp. 1-48.

[8] H. Chen, C. E. Beaudoin, T. Hong, ''Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors,'' *Computers in Human Behavior*, vol. 70, pp. 291-302, 2017, doi: 10.1016/j.chb.2017.01.003.

[9] E. R. Leukfeldt and M. Yar, ''Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis,'' *Deviant Behavior*, vol. 37, no. 3, pp. 263-280, 2016, doi: 10.1080/01639625.2015.1012409.

[10] N. Martin and J. Rice, ''Cybercrime: Understanding and addressing the concerns of stakeholders,'' *Computers & Security*,'' vol. 30, no. 8, pp. 803-814, 2011, doi: 10.1016/j.cose.2011.07.003.

[11] M. M. Singh and A. A. Bakar, ''A Systemic Cybercrime Stakeholders Architectural Model,'' *Procedia Computer Science*, vol. 161, pp. 1147-1155, 2019, doi: 10.1016/j.procs.2019.11.227.

[12] Z. Zulkefli, M. M. Singh, and N. H. A. H. Malim, ''Advanced Persistent Threat Mitigation Using Multi Level Security-Access Control Framework. In: Gervasi O. et al. (eds),'' *Computational Science and Its Applications--ICCSA 2015. ICCSA 2015. Lecture Notes in Computer Science*, Springer, Cham, vol. 9158, pp. 90-105, 2015, doi: 10.1007/978-3-319-21410-8_7.

[13] B. V. Solms, ''Information Security-A Multidimensional Discipline,'' *Computers & Security*, vol. 20, no. 6, pp. 504-508, 2001, doi: 10.1016/S0167-4048(01)00608-3.

[14] R. K. Merton, ''Social Structure and Anomie, ''*American Sociological Review*, vol. 3, no. 5, pp. 672-682, Oct. 1938, doi: 10.2307/2084686.

[15] L. E. Cohen and M. Felson, ''Social change and crime rate trends: a routine activity approach,'' *American Sociological Review*, vol. 44, pp. 588-608, 1979, doi: 10.2307/2094589.

[16] D. B. Cornish and R. V. Clarke, ''*The reasoning criminal: Rational choice perspectives on offending*, New York: Springer-Verlag, eds. 1986.

[17] R. L. Akers, ''*Social Learning and Social Structure: A General Theory of Crime and Deviance*,'' Boston, MA: Northeastern University Press, 2011.

[18] M. Gottfredson and T. Hirschi, ''*A general theory of crime*,'' Stanford, CA: Stanford University Press, 1990.

[19] L. Kohlberg, ''*The Psychology of Moral Development: The Nature and Validity of Moral Stages (Essays on Moral Development*,'' Harper & Row, 1984.

[20] A. Bandura and D. C. McClelland, ''*Social learning theory*,'' Englewood Cliffs, NJ: Prentice Hall, 1977.

[21] R. Volti and W. F. Ogburn, "Social Change with Respect to Culture and Original Nature," *Technology and Culture*, vol. 45, no. 2, pp. 396-405, Apr. 2004.

[22] A. Goldsmith and R. Brewer, ''Digital drift and the criminal interaction order, ''*Theoretical Criminology*, vol. 19, no. 1, pp. 112-130, 2015, doi: 10.1177/1362480614538645.

[23] R. V. G. Clarke and M. Felson, ''*Routine activity and rational choice*, New Brunswick: Transaction Publishers, Inc, vol. 5, 1993.

[24] M. Felson and R. L. Boba, ''Crime and everyday life: Insight and implications for society. Thousand Oaks: Pine Forge Press, 1994.

[25] ASEAN, ''Treaty of Amity and Cooperation in Southeast Asia Indonesia,'' 24 February 1976. Retrieved 20 Nov 2016. [Online]. Available: http://asean.org/treaty-amity-cooperation-southeast-asia-indonesia-24-february-1976/. Accessed November 2016.

[26] ASEAN, ''Joint Communique of the Fourth ASEAN Ministerial Meeting on Transnational Crime (AMMTC), Bangkok, 2004. [Online]. Available: http://asean.org/joint-communique-of-the-fourth-asean-ministerial-meeting-on-transnational-crime-ammtc-bangkok/. Accessed November 2016.
[27] ASEAN, ''ASEAN ICT Masterplan,'' 2015 Completion Report. Jakarta: ASEAN Secretariat.
[28] ASEAN, ''ASEAN Telecommunications and IT Ministers Meeting (TELMIN),'' 2016, Retrieved 20 Nov 2016. [Online]. Available: http://asean.org/asean-economic-community/asean-telecommunications-and-it-ministers-meeting-telmin/. Accessed November 2016.
[29] ASEAN Regional Forum (ARF), ''ASEAN Regional Forum Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyberspace,'' 2016, Retrieved 20 Nov 2016. [Online]. Available: http://www.mofa.go.jp/region/asia-paci/asean/conference/arfstate0607-3.html. Accessed November 2016.
[30] O. S. L. Tan, R. G. Vergara, R C. Phan, S. Khan, and N. Khan, ''Cybersecurity Laws in Malaysia,'' In *Encyclopedia of Criminal Activities and the Deep* Web, IGI Global, 2020, pp. 435-448, doi: 10.4018/978-1-5225-9715-5.ch030.
[31] R. N. M. Shariff, ''Regulatory Framework in Cyber Crime Laws Proceedings of International Conference on E-Commerce,'' 2005, pp 194-199.
[32] M. S. b. Hashim, ''Malaysia's National Cyber Security Policy: The country's cyber defence initiatives,'' *2011 Second Worldwide Cybersecurity Summit (WCS)*, London, UK, 2011, pp. 1-7.
[33] Z. Zulkefli, M. M. Singh, A. R. M. Shariff, and A. Samsudin, ''Typosquat Cyber Crime Attack Detection via Smartphone,'' *Procedia Computer Science*,'' vol. 124, pp. 664-671, 2017, doi: 10.1016/j.procs.2017.12.203Z.
[34] Z. Yunos, R. Ahmad, S. H. Suid, and Z. Ismail, ''Safeguarding Malaysia's critical national information infrastructure (CNII) against cyber terrorism: Towards development of a policy framework,'' *2010 Sixth International Conference on Information Assurance and Security*, Atlanta, GA, USA, 2010, pp. 21-27, doi: 10.1109/ISIAS.2010.5604182.
[35] Malaysia Computer Emergency Response Team (MyCERT). [Online]. Available: https://www.mycert.org.my.
[36] J. Wolff, ''The Real Reasons Why Cybercrimes May Be Vastly Undercounted,'' 2018. [Online]. Available: https://slate.com/technology/2018/02/the-real-reasons-why-cybercrimes-are-vastly-underreported.html.
[37] Telegraph UK, ''Top 10 technology highlights of 2009,'' 2009. [Online]. Available: https://www.telegraph.co.uk/technology/6817359/Top-10-technology-highlights-of-2009.html.
[38] S. Richmond, E. Barnett, and M. Warman, ''Top 10 technology highlights of 2010,'' *Telegraph UK*, 2010. [Online]. Available: https://www.telegraph.co.uk/technology/8216648/Top-10-technology-trends-of-2010.html.
[39] S. Richmond, M. Warman, C. Williams, and E. Barnett, ''Technology trends of 2011: year in review, ''*Telegraph UK*, 2011. [Online]. Available: https://www.telegraph.co.uk/technology/news/8956806/Technology-trends-of-2011-year-in-review.html.
[40] P. Singh, P. Tiwari, S. Singh, ''Analysis of Malicious Behavior of Android Apps,'' *Procedia Computer Science*, vol. 79, pp. 215-220, 2016, doi: 10.1016/j.procs.2016.03.028Get.
[41] N. P. Owoh, M. M. Singh, and Z. F. Zaaba, ''Automatic Annotation of Unlabeled Data from Smartphone-Based Motion and Location Sensors,'' *Sensors*, vol. 18. no. 7, p. 2134, 2018, doi: 10.3390/s18072134.
[42] N. P. Owoh and M. Mahinderjit Singh, ''Applying Diffie-Hellman Algorithm to Solve Key Agreement Problem in Mobile Blockchain based Sensing Applications,'' *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 10, no. 3, pp. 59-68, 2019.
[43] Pius Owoh N, Mahinderjit Singh M., "SenseCrypt: A Security Framework for Mobile Crowd Sensing Applications," *Sensors*, vol. 20, no. 11, p. 3280, 2020, doi: https://doi.org/10.3390/s20113280.
[44] Z. Zulkefli and M. M. Singh, ''Sentient-based Access Control model: A mitigation technique for Advanced Persistent Threats in Smartphones,'' *Journal of Information Security and Applications*, vol. 51, p. 102431, April 2020, doi: 10.1016/j.jisa.2019.102431.
[45] X. Du, D. Shan, K. Zeng, and L. Huie, ''Physical layer challenge-response authentication in wireless networks with relay,'' *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, 2014, pp. 1276-1284, doi: 10.1109/INFOCOM.2014.6848060.
[46] L. L. Bann, M. M. Singh, and A. Samsudin, ''Trusted Security Policies for Tackling Advanced Persistent Threat via Spear Phishing in BYOD Environment,'' *Procedia Computer Science*, vol. 72, pp. 129-136, 2015, doi: 10.1016/j.procs.2015.12.113.
[47] L. Barreto, A. Celesti, M. Villari, M. Fazio, and A. Puliafito, ''An authentication model for IoT clouds,'' *2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, 2015, pp. 1032-1035, doi: 10.1145/2808797.2809361.
[48] B. Koshy, N. Mistry, and K. Jain, ''Chameleon Salting: The New Concept of Authentication Management. In: *Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems*, vol 51, pp. 323-337, 2016, Springer, Cham, doi: 10.1007/978-3-319-30927-9_32.
[49] S. Kim and T. Cho, ''A Study on Vulnerabilities of Linux Password and Countermeasures,'' In *Advances in Computer Science and Ubiquitous Computing*, Springer, Singapore, 2021, pp. 61-67, doi: 10.1007/978-981-15-9343-7_9.
[50] S. Wang, Y. Zhang, and Y. Zhang, ''A Blockchain-Based Framework for Data Sharing with Fine-Grained Access Control in Decentralized Storage Systems,'' in *IEEE Access*, vol. 6, pp. 38437-38450, 2018, doi: 10.1109/ACCESS.2018.2851611.