Cyberattacks and data breaches in Indonesia by Bjorka: hacker or data collector?

Tole Sutikno[1], Deris Stiawan[2]
[1]Department of Electrical Engineering, Faculty of Industrial Tech., Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2]Department of Computer Engineering, Faculty of Computer Science, Universitas Sriwijaya, Palembang, Indonesia

Article Info

Article history:

Received Sep 22, 2022
Revised Sep 27, 2022
Accepted Sep 30, 2022

Keywords:

Cyber-attack
Cyber-security
Hacker
Security hole
Vulnerability

ABSTRACT

Recently, the public has been shocked by the mysterious figure of Hacker Bjorka. Bjorka hacked Indonesian officials. Bjorka leaks Indonesia's General Election Commission (KPU) data. This raises a significant red flag concerning Bjorka's ability to "disrupt" circumstances that are harmful to a large number of individuals, including his alleged action of leaking the personal data of influential state officials. Expert Putra Aji Adhari says Bjorka isn't a hacker. Aji Putra stated that Bjorka is a team. He, who has been invited to communicate with NASA, is sure Bjorka is still in Indonesia. Putra told Bjorka's hacking steps. Ardi Sutedja declared Bjorka isn't a person, his pattern mirrored a hacking group's. Sutedja knew Bjorka was Indonesian. Domestic targets, attacks, and mastery are evidences. On the other hand, Wiryana, as a hacker's handler, said that Bjorka is not a real hacker but rather a data collector. Ismail Fahmi says that a hacker like Bjorka uses a VPN to get to a server without leaving any traces. Bjorka might have come from Indonesia. One sign is that Bjorka's use of English is similar to how most Indonesians talk.

Corresponding Author:

Tole Sutikno
Department of Electrical Engineering, Faculty of Industrial Technology, Universitas Ahmad Dahlan
4th UAD Campus, Ahmad Yani St. (Southern Ring Road), Tamanan, Yogyakarta 55191, Indonesia
Email: tole@te.uad.ac.id

1. INTRODUCTION

The first time Indonesia heard of the hacker now known as Bjorka was at the beginning of September, when news of a massive data leak broke. The passwords for registering some 1,3 billion SIM cards were stolen and offered for sale on a dark web marketplace. The data was collected in part as a result of a 2017 legislation reform in Indonesia that required everyone using an Indonesian SIM card to register it in their name using their identity card, known as a KTP, and their family card, known as a KK. If the leaks had ended there, or if Bjorka-who claim to have taken their name from the Icelandic singer Bjork-had disclosed other internet data for purported financial gain, maybe the story would not have gained so much attention. In the weeks after the data was released, however, Bjorka has gained a cult following online because of his unique personal history and a series of fights with an Indonesian government that is getting more and more angry [1].

The mysterious persona of Hacker Bjorka has been the source of widespread consternation among the general community. Bjorka suddenly appeared and leaked data on top officials in Indonesia. Who exactly is Bjorka? What is the motivation behind Bjorka's surprise attack against the Indonesian government through cyberspace? What are its intentions and goals? These questions continue to bother Indonesian people. Moreover, along with the times, community activities are becoming increasingly inextricably linked to personal data in digital form. Based on Putra Aji Adhari's opinion as a bug hunter and cyber security professional, Bjorka is not a hacker. The name Bjorka denotes a team that works together to attack and leak public data through both government and non-government sites. "But what I read in the Bjorka news is that it's a team," said Putra Aji Adhari. Suppose Bjorka leaked data from Indonesia's General Election Commission (KPU). Then, two months after that, he leaked more data. "In my opinion, this doesn't make sense," he continued. He also said that Bjorka's hacking was too fast on his own. Because to observe the data that is raised to other data needs to take months. "I think it's too soon (Bjorka leaked data to other data if he was alone)," he said. However, this young man, who has been invited to communicate with the United States NASA agency since the age of 15, is sure that the figure of Bjorka is still in Indonesia, not abroad, as the information circulated. "This is the conclusion that I draw from what is circulating on the internet and speculation from the public." "Many people tweet on Twitter, and the way he looks like an Indonesian," he said. "But we have to wait for a statement from the government," he explained [2].

On the other hand, Putra also leaked Bjorka's steps in hacking the data. There are five processes in hacking information; the first is information gathering; the second is scanning or organizing; the third is exploitation; the fourth is reporting; and the last is mitigation. He explained and revealed that Bjorka's hacking had already entered the exploitation stage. "The exploitation is usually when we find a security hole, then we take advantage of the weakness to upload a backdoor" (software used to access systems, applications, or networks without having to handle the authentication process), he explained. Putra said that the weakness in question is that hackers only develop applications. He made a website but did not pay attention in terms of security [2].

2. BJORKA'S TELEGRAM

A young guy from Madiun, East Java, with the initials MAH, has been listed as a suspect in the Bjorka hacking case. MAH has been labeled as a suspect because of his alleged role in assisting the hacking group Bjorka in the spread of personal data relating to the incident. Inspector General Dedi Prasetyo, who heads up the Public Relations Division of the National Police, said that MAH served as the administrator of the Bjorkanism Telegram chat group application. MHA disseminated private information on a variety of Indonesian government officials using his cellphone and the messaging service Telegram. According to Dedi Prasetyo, "Yes, in such a system" refers to the dissemination of information via the use of mobile phones. Regarding the identification of the possible MAH, Dedi has not supplied any more information at this point. On the other hand, he said that MAH was not being held and that she was required to file a report. "The suspect is obligated to report and comply with the information from the Timsus," Dedi elaborated more on the matter [3].

Previously, the Indonesia Coordinating Minister for Political, Legal, and State Affairs, Mahfud MD, said that the Indonesia State Intelligence Agency (BIN) and the Indonesia National Police had the hacker known as Bjorka under their control. Mahfud said that the identity of Bjorka has not been revealed to the general public at this time, in response to a question about the identity of Bjorka. It will not be feasible to make any announcements on who and where specifics are at this time. Mahfud continued, "We already have the capability to track each and every one of them" [4].

3. BJORKA'S TWITTER

Despite repeated account bans, Bjorka has continued to publish stuff on Twitter, doxxing a number of ministers and politicians in Indonesia and making fun of others. Bjorka has criticized politicians for, among other things, the growing cost of petrol, which has sparked demonstrations throughout the nation. This has given the mysterious person a sort of Robin Hood status as a stand-in for the people holding the government accountable, especially after they threatened to release a database of information about Pertamina, the state-owned oil and gas company of Indonesia, that was likely obtained through hacking. Bjorka also stated that their "friend" had left Indonesia as a result of the "1965 policy" - an apparent allusion to the anti-communist purges of 1965 and 1966, which caused thousands of intellectuals, academics, activists, and political figures from Indonesia to leave the nation after mass executions of people thought to be communist sympathizers. According to estimates, between 500,000 and 1 million individuals perished during the anti-communist purges. Although hard to confirm, this interesting history gave Bjorka's most recent hacks a very political flavor. According to analysts, Bjorka's antics reveal the underlying issue of Indonesia's lack of cybersecurity readiness in addition to the internet mischief. The National Cyber and Crypto Agency (BSSN), the Ministry of Communication and Information (Kominfo), the Indonesian National Police (Polri), and the Indonesian Intelligence Agency (BIN) have been assembled into an Indonesian government task force for data protection, which Krisetya claims runs counter to the agency's founding principle of ending duplication of authority among government institutions dealing with cybersecurity issues. He said, "The government's decision to establish yet another body demonstrates how disjointed our cybersecurity governance is and that none of the current organizations has the coordinating capacity to react to cyber events [5].

4. CYBERSECURITY EXPERTS' VIEWS

In addition, the assertion that Bjorka is not a single person has been validated by Ardi Sutedja, who is an expert in cyber defense. According to him, Bjorka is, in fact, a group that is solely interested in gaining notoriety. Ardi Sutedja reached the conclusion that Bjorka was an Indonesian national on the basis of the identification that was made. This can be seen from a pattern of targets, attacks, and mastery over practical issues, all of which do not reflect as a playing group in the international realm. Ardi Sutedja, a specialist in computer security, was asked about the entity and responded, "I believe this is a group." He continued by saying, "The pattern that Bjorka did is very similar to the pattern of the hacker group, which until now has never been found in the face of who we don't know," he continued. They also said the most famous hacker is anonymous, which is where Bjorka performs a similar hacking pattern. "Anonymous is defending the method, which is no different from Bjorka's," he explained. "The pattern is the same in hacking out the data, Anonymous continues to not ask for economic motivation, it's very similar, yes," he continued. Even Ardi Sutedja mentioned that there is something special about Bjorka, and that something is the fact that the hacker is not from another country. The reason for this is that Bjorka brought the matter up in the nation. Unlike Anonymous, whose identity on a global scale is still a mystery to this day, we don't know anything about them. He went on to explain that "in the end, what took place in Bjorka is like that" (anonymous). "There is no way we can find out who did it." Additionally, Ardi Sutedja shed light on the fact that additional research into the identities of the two hackers is still in progress. Because finding it is a process that takes some time and is fairly drawn out. "We can't just make the assumption that this case is like that; it's not that cut and dried. We require expertise and knowledge from a broad range of fields. Who knows? Only time will tell "he said [6].

The cyber and ICT expert from Universitas Brawijaya (UB), Herman Tolle, is of the opinion related to the viral hacker Bjorka, who leaked the personal data of officials to the internet. He believes Bjorka has connections with Indonesian hackers. Herman explained that if Bjorka had hacked for fun, a small amount of personal data could be leaked. "My analysis could be that at first it was from outside. The original hacker could be from abroad. But what is clear is that he has connections to Indonesians, so he knows or wants to break into which or whose data. maybe," said Herman Tolle. Actually, there is a forum like that. Hackers have a community on the web. There is a dark web. It contains hackers sharing information, including selling data. Maybe this is a personal opinion, but there is information sharing, trying to break into existing applications, and it turns out it works. "Something can be broken into," he said. If I analyze that recently a lot of data has been breached, including at UB itself, the hackers are actually insiders (Indonesians), not from abroad but Indonesians themselves. They try to break into it. If it's outsiders, there is no urgency, "added the lecturer at the Faculty of Computer Science (Filkom) Universitas Brawijaya [7].

According to I Made Wiryana, a cybersecurity competency specialist, Bjorka was merely a data collector and not a true hacker. The actions taken by Hacker Bjorka were not typical of those taken by hackers. I Made Waryana suggests that an interest in the operational specifics of a system is a common trait among hackers. He will investigate the system in an effort to identify any vulnerable spots or weak spots in it. However, it will not publish the findings of its investigation. There is no technical curiosity. According to I Made Wiryana, "Yes, it's possible that he employs social engineering in the process of gathering it; nevertheless, as a technical hacker, he doesn't need to have that expertise" [8].

Ismail Fahmi, a social media analyst and founder of Drone Emprit, stated that a savvy hacker would use a virtual private network (VPN) to access a server without leaving any traces. This is performed by hackers such as Bjorka. I'm presuming the hacker is intelligent; he has attempted to delete all traces. If we access a server from our mobile devices, it is immediately captured. For example, opening a Twitter login with a username such as Bjorka from an IP address in Indonesia, it will be caught," said Fahmi. For the purpose of erasing traces, hackers will utilize a VPN from outside. It will utilize VPNs from a variety of nations, not just one. But Bjorka is clever; he previously accessed it over a VPN. He uses one foreign VPN, then uses another VPN, continues to several places of entry and entry, then accesses the target. It is common knowledge that access is not restricted to Indonesia "explained Fahmi. According to him, Bjorka may have originated in Indonesia. One indicator is Bjorka's usage of the English language. Bjorka's English is comparable to the normal communication style of Indonesians [9].

5. WHO IS BJORKA?

The Indonesian House of Representatives (DPR) Commission I has decided to raise the budget for the Indonesia National Cyber and Encryption Agency (BSSN) to Rp 624 billion in 2023. The enhanced budget ceiling was agreed upon to assist the agency in providing stronger security against cyberattacks like the recent Bjorka intrusions. Hinsa Siburian, CEO of BSSN, expressed gratitude for the budget increase approval. "After we approve it and pass it over to the House Budget Committee (Banggar), where the draft would be developed again," he continued, "it would be read out during an official plenary after that." The BSSN is researching Bjorka's identification, assisted by a specialized team from numerous governmental authorities. Because it is more technical, I believe they (Bareskrim) will be able to explain it more later. So, we'll simply have to wait since this is about digital forensics, "BSSN Head Hinsa Siburian said. But when Hinsa was asked about Bjorka's identity, whether the offender was from inside or outside the nation, and if Bjorka was a single individual or a group, she only grinned and refused to give any information. "As for that question," he continued, "we're looking into that right now." The administration has already recognized that data breaches have occurred. Johnny G. Plate, Indonesia's Minister of Communications, said that the information being passed around was old general data [10].

6. HACKER TYPES, MOTIVATIONS AND STRATEGIES

Samuel Chng and his colleagues [11] have distinguished a total of thirteen distinct categories of hackers. These categories include newbies, students, thugs, online sex offenders, old guards, insiders, petty thieves, hacktivists, digital pirates, professionals, crime facilitators, crowdsourcers, and nation states. In addition to this, the researchers came up with seven essential reasons for hacking (curiosity, recreation, notoriety, financial, sexual impulses, revenge, and ideology) as shown in Table 1. In addition to this, they have documented the strategies that are used by every class of hacker.

Students hack simply to obtain knowledge. They're motivated by curiosity. Novice hackers are less proficient and mainly rely on internet toolkits developed by others. Other terms for this sort of hacker are script kiddies, rookies, and system difficulties. Novices' motivations include curiosity, notoriety, and recreation. Students may also utilize existing codes/scripts like novices, but with minor modifications, to explore and analyze vulnerabilities in web servers, databases, and cloud storage servers. Novices reuse codes/scripts/malware obtained on the internet and dark web with little change. They lack a comprehensive plan of attack measures to attain their aim. In many circumstances, they aren't attentive enough to mask their internet trails to evade the law [11], [12].

Cyberpunks are low-to-medium-skilled hackers who wreak havoc for fun. They are motivated by financial gain, notoriety, revenge, and recreation. Online sex offenders are sexually motivated individuals who misuse the internet to engage in sexually deviant behaviours with children. Old guards, like students, are non-malicious hackers who have no regard for personal privacy and include white hats, sneakers, grey hats, and tourists. They are motivated by curiosity, notoriety, recreation, and ideology. Cyberpunks may use existing codes/scripts but with some modifications or write their own ones to suit their goals. They may use attack vectors to cause damage to victim systems, such as bricking PCs or embedded devices, and carrying out DoS attacks to deny legitimate users access to the victim machines. Other attack vectors such as phishing, spamming, SQL injection, simple malware/ransomware may also be used for stealing credit card information, unauthorized account transactions, identity fraud, and bitcoin theft [11].

Insiders are unhappy current or ex-employees who misuse their access. Internals, user malcontents, and business raiders are driven by money, retribution, and ideology. Petty thieves commit crimes online for financial gain and retribution. Extortionists, scammers, fraudsters, thieves, and digital thieves. Digital pirates illegally copy, distribute, download, or sell copyrighted materials. They're cash-driven. Insiders exploit confidential corporate data (e.g., account passwords, security policies, system vulnerabilities) to conduct attacks or sell it to Dark web customers and competitors. Petty thieves who are financially motivated use attack vectors such as trojans, keylogging, phishing, and ransomware, which are easily available online or in hacking forums, to gain credit card or bank account details of users or blackmail users into transferring a ransom amount in bank currency or cryptocurrency [11].

Crime facilitators provide cybercriminals the tools and know-how to execute complex attacks. Professionals operate as hired shooters or to further their criminal business. Highly proficient nation state hackers destabilize, disrupt, and destroy a nation or government's systems and networks. Profit, revenge, and ideology drive them. Crowdsourcers tackle problems using questionable means and dubious intentions. Hacktivists, sometimes called political activists and ideologists, use their technical abilities for political change. Notoriety, retribution, leisure, and ideology inspire them [11].

It is unknown whether the hacker known as Bjorka is an Indonesian citizen or even if they are present in the country, which might be problematic if the authorities seek to bring charges against them [5]. If Bjorka is not in Indonesia, they must be deported, which is a difficult process. If extradition is requested, it will depend on whether Bjorka is living in a nation with which Indonesia has an extradition agreement and if Indonesian authorities have a strong enough case to support extradition. This ambiguity has increased the controversy around the case. Improved awareness and a change in attitudes are two things that must happen, among other things. The Indonesian government needs to take more proactive measures to address potential consequences of already leaked personal data, including the possibility that criminals may use names, phone numbers, and dates of birth-among other information-for online fraud, harassment, abuse, or even cyberterrorism.

Table 1. Hacker types, motivations and strategies

No	Hacker Types	Motivations	Strategies
1	Students	C	May use existing codes/scripts like novices but with some modifications to experiment and study vulnerabilities in systems. Likely to report the vulnerabilities.
2	Online sex offenders (Cyber Predators, or Pedophiles)	S	Befriend prospective victims on Facebook or other social media platforms.
3	Digital pirates (Copyright Infringers)	F	Directly or indirectly steal and leak copyrighted content.
4	Crime facilitators (Supporters)	F	May provide criminals with cybercrime-as-a-service by assisting them with phishing campaigns, renting out malware and botnets, and so on.
5	Petty thieves (Extortionists, Scammers, Fraudsters, or Thieves)	F, Rv	Use attack vectors like as trojans and ransomware that are widely available on the internet to obtain credit card or bank account information.
6	Professionals (Black Hats, Elites, Criminals, Organized Crime, or Information Brokers)	F, Rv	Use the full range of attack vectors and custom code/scripts to carry out sophisticated attacks. Make sure not to leave any online traces.
7	Insiders (Internals, User Malcontents, or Corporate Raiders)	F, Rv, I	Use private information about a company's cyberinfrastructure to attack the company or sell that information. May transfer sensitive company data to their own devices, access company databases, servers, and cloud storage.
8	Nation states (Information Warriors, Cyber Terrorists, Cyber Warriors, State Actors, or State-Sponsored Networks)	F, Rv, I	Perform sophisticated attacks following a series of stages. First, they gain access to a target network, second, they gain a foothold by installing malware on a system, third, they try to gain administrative rights, fourth, they identify and prepare valuable data for exfiltration, fifth, they persist and continue above process for a long time.
9	Old guards (White Hats, Sneakers, Grey Hats, or Tourists)	C, N, Rc, I	Use customized codes, scripts, and penetration testing tools to find holes in systems that are already in place. Malicious hackers can be tracked down using cyber forensic techniques and professional honeypots to find new malware. Add both white and gray hats.
10	Thugs (Cyberpunks, Crashers, or Crackers)	F, N, Rv, Rc	May use existing codes/scripts but with some modifications or write their own ones. Attack vectors include bricking to cause damage to victim systems, exploiting bugs in software running on victim's devices, and carrying out Denial of Service (DoS) attacks. Focused on garnering public and media attention.
11	Hacktivists (Political Activists, or Ideologists)	N, Rv, Rc, I	Employ attack vectors such as SQL injection, web server misconfiguration to take over databases and leak their contents, deface high-profile websites, and disable widely-used public services.
12	Crowdsourcers	N, Rv, Rc, I	Join forces and share their skills to do things like make new malware, manage botnets, and so on.
13	Newbies (Novices or Script Kiddies)	C, N, Rc, I, S	Utilize already discovered programs, scripts, or malware from the internet. Do not have an adequate plan of action in terms of the procedures necessary to launch an attack. They have not been sufficiently cautious to hide their web trails.

C: Curiosity, F; Financial, N: Notoriety, Rv: Revenge, Rc: Recreation, I: Ideology, and S: Sexual Impulse

7. CONCLUSION

Bjorka's media sensation and hacking have increased awareness about the necessity of personal data protection regulations. If the protection scheme was not prepared from scratch, data leaks, cybercrime, and hacking would be serious issues in Indonesia and around the world. Concerns about the information Bjorka possesses and how it was leaked are understandable, but this example reveals deeper flaws in Indonesia's approach to cybersecurity over time. Everything these days is data-driven. All governments and private parties today are competing to collect data on a large scale. These cyber-attacks frequently target the government, private sector, and general public. The fact that billions of regular people's data in September 2022 may have been leaked in the Bjorka attacks because they were not protected must be fixed right away. Comprehensive laws on the collecting and storage of personal information, as well as accountability measures that public or private entities must take in the event of a breach, are critical.

REFERENCES

[1] L. Yulisman, “Indonesia hunts for Bjorka, hacker selling 1.3b SIM card users’ data, taunting officials,” *The Straits Times*, 2022. https://www.straitstimes.com/asia/se-asia/indonesia-hunts-for-bjorka-hacker-selling-13b-sim-card-users-data-taunting-officials (accessed Sep. 22, 2022).

[2] H. Nguyen, “The Long Road to Hunting Bjorka, An Effective Way to Dismantle the Personal Data Scrambler,” *Newsdelivers*, 2022. https://www.newsdelivers.com/2022/09/21/the-long-road-to-hunting-bjorka-an-effective-way-to-dismantle-the-personal-data-scrambler/ (accessed Sep. 22, 2022).

[3] R. Hidayat, “Man from Madiun Previously Suspected as Bjorka Charged Under Article from ITE Law,” *Jakarta Daily*, 2022. https://www.jakartadaily.id/tech-media/pr-1624802096/man-from-madiun-previously-suspected-as-bjorka-charged-under-article-from-ite-law (accessed Sep. 22, 2022).

[4] R. Hidayat, “Mahfud MD: Bjorka’s Identity is in the Hands of the National Police and BIN,” *Jakarta Daily*, 2022. https://www.jakartadaily.id/tech-media/pr-1624733610/mahfud-md-bjorkas-identity-is-in-the-hands-of-the-national-police-and-bin (accessed Sep. 22, 2022).

[5] A. Llewellyn, “Bjorka, the Online Hacker Trying to Take Down the Indonesian Government,” *The Diplomat*, 2022. https://thediplomat.com/2022/09/bjorka-the-online-hacker-trying-to-take-down-the-indonesian-government/ (accessed Sep. 23, 2022).

[6] N. Janti, “‘Hacktivist’’ polarizes Indonesian netizens after data breach spree,’” *TheJakartaPost*, 2022. https://asianews.network/hacktivist-polarizes-indonesian-netizens-after-data-breach-spree/ (accessed Sep. 22, 2022).

[7] A. Midaada, “Viral Hacker Bjorka Leaks Official Data, Universitas Brawijaya IT Expert Uncovers His Figure (in bahasa viral hacker bjorka bocorkan data pejabat pakar it universitas brawijaya bongkar sosoknya),” *iNewsJatim.id*, 2022. https://jatim.inews.id/berita/viral-hacker-bjorka-bocorkan-data-pejabat-pakar-it-universitas-brawijaya-bongkar-sosoknya (accessed Sep. 22, 2022).

[8] Virginia, “Bjorka is more of a cracker, not a hacker, this is how he operates unloading data,” *Indonesia Post English*, 2022. https://indonesia.postsen.com/trends/227604/Bjorka-is-more-of-a-cracker-not-a-hacker-this-is-how-he-operates-unloading-data.html (accessed Sep. 22, 2022).

[9] D. Rizky, “Drone Emprit Analysis: Bjorka Hacker Allegedly Indonesian (in bahasa analisa drone emprit hacker bjorka diduga orang indonesia),” *inilah.com,* 2022. https://www.inilah.com/analisa-drone-emprit-hacker-bjorka-diduga-orang-indonesia (accessed Sep. 22, 2022).

[10] E. Team, “Protect Indonesia from Cyber Attacks, The Indonesian House Of Representatives Agreed To A BSSN Budget Of IDR 624 Billion,” *VOI*, 2022. https://voi.id/en/news/211970/protect-indonesia-from-cyber-attacks-the-indonesian-house-of-representatives-agreed-to-a-bssn-budget-of-idr-624-billion (accessed Sep. 23, 2022).

[11] S. Chng, H. Y. Lu, A. Kumar, and D. Yau, “Hacker types, motivations and strategies: A comprehensive framework,” *Comput. Hum. Behav. Reports*, vol. 5, p. 100167, 2022, doi: https://doi.org/10.1016/j.chbr.2022.100167.

[12] D. Riley, “15-year-old script kiddie arrested in TalkTalk hacking investigation,” 2015. https://siliconangle.com/2015/10/27/15-year-old-script-kiddie-arrested-in-talktalk-hacking-investigation/ (accessed Sep. 23, 2022).

BIOGRAPHIES OF AUTHORS

Tole Sutikno is a lecturer in the Electrical Engineering Department at the Universitas Ahmad Dahlan (UAD), Yogyakarta, Indonesia. He received his B.Eng., M.Eng., and Ph.D. degrees in Electrical Engineering from Universitas Diponegoro, Universitas Gadjah Mada, and Universiti Teknologi Malaysia, in 1999, 2004, and 2016, respectively. He has been an Associate Professor at UAD, Yogyakarta, Indonesia since 2008. He is currently the *Editor-in-Chief* of the Bulletin of Electrical Engineering and Informatics and the Head of the Embedded Systems and Power Electronics Research Group. His research interests include the fields of digital design, industrial applications, industrial electronics, industrial informatics, power electronics, motor drives, renewable energy, FPGA applications, embedded systems, artificial intelligence, intelligent systems, information systems, and digital libraries. He can be contacted by email at tole@ee.uad.ac.id.

Deris Stiawan, M.T., Ph.D received his Ph.D. degree in Computer Engineering from Universiti Teknologi Malaysia, Malaysia in 2014. He is currently an Associate Professor with the Department of Computer Engineering, Faculty of Computer Science, Universitas Sriwijaya. He also Manager of Communication Network, Enterprise & Information Security (COMNETS) Research Group Universitas Sriwijaya, and Technical Consultant for the Indonesia Ministry of Education, Culture, Research, and Technology. His research interests include computer networks, intrusion detection/prevention systems, and heterogeneous networks. He can be contacted at email: deris@unsri.ac.id.