International Journal of Society Reviews (INJOSER) e-ISSN: 3030-802X
Vol. 2 No. 11, September 2025, pages: 2245~2255

# CURRENT THREATS TO CYBER SECURITY: STRATEGIES FOR PROTECTING PERSONAL DATA IN THE DIGITAL AGE

**Gunawan Widjaja**
Senior Lecturer Faculty of Law Universitas 17 Agustus 1945 Jakarta
widjaja_gunawan@yahoo.com

**Abstract**

The development of digital technology has brought convenience to various aspects of life, but on the other hand, it has also given rise to increasingly complex cyber security threats. Personal data is now a prime target for attacks because it has high economic value and can be exploited for illegal purposes. The latest threats include phishing, malware, ransomware, data leaks, attacks on Internet of Things devices, and digital manipulation using *deepfake* technology. The complexity of these threats not only harms individuals, but also impacts organisational security, social stability, and public trust in the digital ecosystem. Therefore, personal data protection strategies are crucial in facing the ever-evolving dynamics of cyber attacks. Effective strategies for protecting personal data include the use of two-factor authentication, data encryption, regular system updates, and the use of artificial intelligence for early threat detection. In addition, improving public digital literacy plays a central role in preventing social manipulation, while legal regulations such as the Personal Data Protection Act are an important foundation for upholding individual privacy rights. With a combination of technology, regulation, and digital awareness, personal data security can be strengthened so that the risk of cyber threats can be minimised. This study provides a comprehensive overview of current threats and offers adaptive mitigation strategies in the digital age.

**Keywords**: Cyber security, digital threats, personal data, privacy protection, encryption, digital literacy, Personal Data Protection Act.

## Introduction

The development of digital technology in the 21st century has brought about major transformations in various aspects of human life, including social, economic, educational, and governmental fields. Daily activities that were previously done manually can now be easily accessed through digital devices connected to the internet (Diskominfo Sukoharjo, 2025) . Banking services, e-commerce transactions, communication, public administration, and even health services are now increasingly digitised and provide high efficiency for the community. However, behind these benefits, the digital era also presents a new vulnerability, namely the threat of cyber security that is increasingly complex, diverse, and difficult to detect early on (P .

Cyber security has become a strategic issue that is not only technical in nature, but also involves social, economic, political, and even geopolitical aspects. Various global reports show a significant increase in cyber attacks, such as data theft, malware attacks, and even digital identity theft (F. Rafiq, 2022) . This increase not only affects

large institutions such as banks and multinational companies , but also targets individuals with personal data stored on various digital platforms. This reality emphasises that everyone is now vulnerable to the risk of digital attacks, where personal data is the main target of cybercriminals (T .

Personal data has a very high value in the modern digital ecosystem. Information such as full names, identity numbers, email addresses, passwords, and online transaction histories can be exploited by irresponsible parties for various illegal purposes, ranging from financial theft to social manipulation. In the context of big data and the information-based economy, personal data is even considered the "new currency" that holds greater value than conventional resources. Therefore, threats to personal data security are a serious issue that not only infringes on individual privacy but also threatens broader social and economic stability. (Elitery, 2024) .

Cyber security threats do not only come in purely technical forms such as malware or computer viruses, but also through psychological manipulation techniques based on social engineering. Phishing, for example, has become a classic but still effective method of tricking users into voluntarily handing over their personal data (S. Slapničar, 2022) . On the other hand, the use of artificial intelligence technology has given rise to new forms of digital threats, such as the use *of deepfakes* to create false identities or the spread of misleading information that has the potential to damage a person's reputation. This shows that the evolution of cyber threats runs parallel to the development of technology itself (Naeem AllahRakha, 2024) .

This situation is exacerbated by the high penetration of Internet of Things (IoT) devices in everyday life. Smart devices such as home security cameras, digital watches, virtual assistants, and household appliances are now connected to the internet, but often have weak security systems. Such vulnerabilities provide opportunities for hackers to exploit security loopholes and gain access to personal data and user activities. Thus, the increasing number of devices connected to the global network will further increase the potential risk of cyber attacks. In addition, large-scale *data breaches* or data leaks are becoming an increasingly frequent phenomenon (Titis Pandan Wangi Reformasi & Hasrul Buamona, 2024) . There have been many cases where the databases of public institutions and private companies have been targeted by hackers, resulting in the personal data of millions of users being spread across the digital space. Cases like these are not only financially damaging, but also cause serious digital trauma to public trust in technology-based services. If left unchecked, this crisis of confidence will hamper the development of the digital ecosystem, which has been expected to support national and global economic growth (SWatini, 2024) .

Indonesia, as one of the countries with the largest number of internet users in the world, also faces the threat of high-intensity cyber attacks. The varying levels of digital literacy among the population, coupled with the rapid penetration of digital services, make the protection of personal data a crucial issue. The phenomenon of

widespread data misuse by irresponsible parties, ranging from online fraud, social media account hijacking, to digital identity theft, shows that cyber threats are no longer just a potential risk, but an ongoing reality (H .

In addressing this issue, the Indonesian government has initiated various regulations related to personal data protection, one of which is through the Personal Data Protection Law (PDP Law). The presence of this regulation is an important milestone in providing a legal basis for enforcing cyber security and protecting individual privacy rights (Aleksandra Kuzior et al., 2024a) . However, the success of its implementation is highly dependent on the synergy between regulations, technology, and public awareness in maintaining personal data security. Therefore, research on current threats and protection strategies is highly relevant to support national efforts in strengthening digital security (W .

Personal data protection strategies not only emphasise technical aspects, such as the use of encryption or dual authentication systems, but also include education and changes in people's digital behaviour. Digital literacy is key to creating users who are agile and critical in the face of social engineering attempts. Without a good understanding, even the most sophisticated technology will remain vulnerable to exploitation, because the biggest weakness in cyber security systems often lies in human negligence. Thus, a comprehensive strategy must include a combination of technological strengthening, legal policies, and community empowerment (F .

Efforts to prevent cyber attacks can also be enhanced through the use of cutting-edge technology based on artificial intelligence and *machine learning*. This technology enables faster detection of threats through analysis of suspicious data patterns and provides early warnings before large-scale attacks occur. The concept of *cyber threat intelligence* developed by various international institutions can also be adopted to increase institutional awareness in protecting the personal data of its users. With this proactive approach, increasingly sophisticated threats can be addressed with more adaptive and preventive strategies (Karier.mu, 2024) .

However, despite the development of various strategies, personal data protection still faces major challenges. Limited resources, low public awareness, and the increasingly widespread nature of digital attacks demand more innovative and systematic solutions. Personal data protection cannot be left solely to the government or digital service providers, but requires the active participation of all stakeholders, including individuals as data owners. Cyber security is essentially a shared responsibility that requires continuous cross-sector collaboration (Csirt BPIIP, 2025) .

Based on this description, this study aims to identify current threats that have the potential to compromise personal data security and formulate effective strategies for protecting data in the digital age. With a comprehensive review, it is hoped that a clear picture of modern cyber attack patterns can be obtained, along with practical recommendations that can be applied by individuals, institutions, and policy makers.

Ultimately, this research not only contributes theoretically to the development of science, but also practically in facing the major challenges of digital security today.

## Research Methods

The research method used in this study was a qualitative approach with a library research method, in which the researcher collected and analysed various secondary sources in the form of current scientific journals, cyber security agency reports, government regulations on personal data protection, and academic articles relevant to the theme of cyber security threats and data protection strategies (Eliyah & Aslan, 2025) . The data was analysed using content analysis to systematically identify the most current types of cyber threats, dominant attack patterns, and personal data prevention and protection strategies that have been proven effective in various contexts. This approach was chosen because it allows researchers to gain a comprehensive, integrative, and critical understanding of cybersecurity issues and offers practical recommendations that can be applied in dealing with the dynamics of digital threats in the modern era (Bolderston, 2008) .

## Results and Discussion

### Current Threats to Cyber Security

Cyber security threats continue to evolve alongside advances in digital technology, which affect almost every aspect of human life. Whereas cyber attacks used to be relatively simple, such as spreading viruses or Trojans to disrupt systems, they have now evolved to become more complex and structured. Modern hackers are able to target weaknesses in networks, software, and human factors, thereby increasing the risk of personal data theft and disruption to digital infrastructure (Reno Andre Permana, 2025) .

One of the most prominent threats is phishing attacks. Phishing uses social engineering to trick users into providing sensitive information, such as passwords, PINs, or credit card details. These attacks are usually carried out via email, instant messaging, or fake websites designed to resemble official platforms. Because users tend to have a high level of trust in convincing appearances, phishing remains one of the most difficult threats to avoid, even though this technique is not new (Abdullah Azizi et al., 2025) . In addition to phishing, ransomware is also a major threat in the digital age. Ransomware is a type of malware that locks or holds the victim's data hostage, with the attacker demanding a ransom to return it. These attacks are becoming increasingly popular due to the large financial gains and the tendency of companies and individuals to pay to restore access to their data. Global ransomware cases, such as *WannaCry,* show how vulnerable digital systems are that are not regularly updated (AYusliwidaka, 2024) .

*Data breaches* are also a common cyber threat to this day. Many public institutions and private companies have been targeted, with millions of users' personal

data stolen and then sold on the *dark* web. Data breaches not only result in financial losses, but also undermine public trust in technology-based services. In the long term, this hinders the pace of digital transformation that many countries are striving for (Graduate BINUS University, 2024) .

Distributed Denial of Service (DDoS) attacks are increasingly being used by attackers to paralyse servers or online applications. By flooding the target with large amounts of data traffic, the system becomes unable to provide normal services. These attacks are often used as a means of sabotage to disrupt business continuity, government, and digital public services. The effects are not only economically damaging but can also disrupt social stability if they target critical infrastructure (DFebriawan, 2024) ).

Cyber security threats also arise through sophisticated malware that can operate silently on users' devices. Modern malware no longer functions solely to damage systems, but also records activities, steals biometric data, and even controls devices remotely. The evolution of malware serves as a reminder that digital threats are increasingly focused on stealing personal and intimate data, rather than merely causing technical damage to computer systems (J .

The emergence of *Advanced Persistent Threats* (APT) shows how cyber threats are now more organised. APTs are usually carried out by experienced hacker groups who are suspected of having support from certain countries. They target not only individuals, but also corporations and government agencies for economic, political and intelligence purposes. APT attacks are long-term, covert and systematic, making them extremely dangerous to national security and global stability. (MF Adhiwisaksana, 2023).

The Internet of Things (IoT) brings enormous benefits with the connectivity of smart devices in everyday life, but it also opens up new gaps in cyber security. Many IoT devices such as CCTV cameras, smart lights, and even health devices do not have adequate security systems. Hackers can exploit these vulnerabilities to take control, spy on user activities, or access sensitive data. As the use of IoT devices increases, so does the potential for threats. (R .

*Deepfake* threats are a new phenomenon in the realm of digital security. This technology is capable of creating fake videos or audio that are very similar to the originals, so they can be used to spread hoaxes, damage reputations, or carry out extortion. Deepfakes can also be used for digital identity theft, where a person's face or voice is used illegally to gain access to biometric-based systems. This creates risks that are increasingly difficult to address with conventional security systems (Ana Sofa Yuking, 2018) .

Cyber attacks on the financial sector are one of the main targets because of the huge economic profits they offer. Digital banking transactions, e-wallets, and fintech services are vulnerable to intrusion if they do not have a multi-layered security system.

Attackers can exploit vulnerabilities in applications, networks, or even user negligence to gain illegal access to funds. This phenomenon requires the financial sector to continuously update its security protocols because attacks are constantly evolving and never stop (RAnggriawan, 2022) . The health sector is also increasingly becoming a target for cybercriminals. Hospitals, clinics, and digital health applications store highly sensitive patient medical data. Attacks on this sector can have fatal consequences, as they are not only related to privacy but also to life safety. If medical data is manipulated or if the healthcare system is paralysed by a cyber attack, the impact can be far more serious than just financial loss (Najamuddin Gani, 2024) .

Attacks on social media and private communication platforms also deserve special attention. There have been many cases of account hacking that have led to digital identity theft, misuse of personal information, and even blackmail (*sextortion*). Given that social media has become an important part of social interaction and a person's public image, the threat of account hacking can damage the reputation and trustworthiness of individuals who fall victim to it, and even disrupt their mental health. In addition to external threats, there are also internal risks or *insider threats,* where employees or parties within an organisation misuse their access to steal data or damage systems. These threats are often more difficult to detect because the perpetrators have legitimate access to the system. In several cases, major data breaches have occurred due to weaknesses in internal oversight, not solely external attacks (Dudy Heryadi et al., 2024) .

The geopolitical context has also reinforced the trend of cyber attacks. Countries have begun to use digital attacks as part of their modern warfare or economic conflict strategies. Cyber warfare can target a country's critical infrastructure, such as power grids, transportation systems, and telecommunications. With increasing tensions between countries, threats to cyber security are now not just a matter of individual criminality, but also part of a larger global strategy (S .

Thus, the current threats to cyber security are diverse and continue to evolve in line with technological advances. Cyber attacks are no longer designed solely to damage computer systems, but also target financial, social, health, and even geopolitical aspects. This complexity requires all parties, from individuals and companies to countries, to raise awareness and build stronger protection systems. Without preparedness to face the latest threats, the risk of personal data loss and multidimensional losses will become increasingly difficult to avoid.

**Strategies for Protecting Personal Data in the Digital Age**

Personal data protection in the digital age requires a comprehensive approach, given that cyber threats are growing and targeting various aspects of modern society. Defence strategies cannot rely solely on technology, but must also involve legal regulations, institutional policies, and individual awareness as data owners. These

efforts require the involvement of all parties, as personal data has become a valuable asset that can be exploited for illegal transactions, identity manipulation, and economic exploitation (R .

The main step that needs to be taken is to implement two-factor authentication or multi-factor authentication (MFA) on every digital platform, especially services that involve finances and sensitive data. MFA adds a layer of security by requiring users to enter an additional verification code in addition to their password, such as an OTP code via SMS or an authenticator app. This strategy is effective in reducing risk because even if the password is successfully hacked, the hacker still cannot access the account without the additional verification code (W .

Data encryption is a fundamental strategy widely used to protect digital information. With encryption, data that is sent or stored can only be read by parties who have the decryption key. This technology is important to apply to personal communications, online transactions, and data storage in cloud services. Without encryption, data can be easily intercepted, accessed, or misused by unauthorised parties during transmission or storage. (MF Asyrofi, 2025) .

Regular software updates are also an important strategy in preventing cyber attacks. Many attacks occur because devices or applications are still using older versions that have security vulnerabilities. Software manufacturers regularly release updates to close these vulnerabilities. Therefore, disciplined *updating of* operating systems, antivirus software, and digital applications is a simple but crucial preventive measure (ST Hossain, 2025) .

Digital literacy among the public needs to be improved because even the most sophisticated security technology will not be effective if users are not aware of the need to protect their personal data. Education about the dangers of phishing, the use of strong passwords, and how to identify fake websites are key priorities in protecting the public from social engineering. The higher a person's level of digital literacy, the less likely they are to fall victim to online manipulation or fraud (Aleksandra Kuzior et al., 2024b) .

Another important strategy is to maintain the security of social media accounts, given that these platforms are one of hackers' favourite targets. Weak passwords are often exploited to hack into personal accounts. Therefore, users are advised to use unique passwords that combine uppercase letters, lowercase letters, numbers, and symbols. Additionally, avoiding the use of the same password for multiple accounts is key to preventing a domino effect if one account is successfully hacked (B .

Digital service providers and institutions have a significant responsibility to protect consumer data. They must implement a clear *cybersecurity framework*, conduct regular audits of their security systems, and use advanced technologies such as next-generation firewalls and intrusion detection systems. In addition, companies must adopt the principle *of privacy by design*, which means ensuring that personal data

protection is taken into account from the early stages of system or application development (ME Susila, 2024) .

The role of government regulation in protecting personal data is vital. Regulations such as the Personal Data Protection Act (PDP Act) in Indonesia provide a legal framework that binds all parties to protect individual privacy. These regulations require digital service providers to be transparent in their use of user data and to give greater control to data owners. Without clear rules, many companies tend to ignore privacy protection in favour of commercial gain (AF Sadeli, 2023) .

International cooperation is also necessary because cybercrime knows no national boundaries. Attacks can originate from abroad and target domestic systems, requiring global synergy to counter the threat. Through international cybersecurity forums, countries can share information on attack patterns, the latest prevention technologies, and legal mechanisms for prosecuting cross-border criminals. This collaboration strengthens cyber resilience at both the national and regional levels (Diskominfo Sukoharjo, 2025) .

At the individual level, data protection strategies can also be implemented by limiting the amount of personal information shared online. Many users are unaware that sharing small details on social media, such as their date of birth, full address, or identity photos, can be exploited for digital identity theft. The principle *of thinking before sharing* is one of the simplest ways to reduce the risk of personal data leaks (P. Swire, 2024) .

The management of personal data storage devices is also very important. Using cloud storage with high security, encrypting external devices, and permanently deleting sensitive data when it is no longer needed are additional strategies to reduce the risk of misuse. In addition, regular data backups also help anticipate data loss due to ransomware attacks that hold important files hostage (F. Rafiq, 2022) .

Personal data protection can also be strengthened through the use of artificial intelligence (AI)-based monitoring technology. AI-based security systems are capable of detecting unusual attack patterns faster than humans. For example, if there is suspicious login activity from an unusual location, the system can immediately issue a warning or even block access attempts before further damage occurs. This technology is particularly relevant for application in the financial, healthcare, and government sectors (T . In addition to technical protection, it is also necessary to instil a culture of digital security in every organisation. Employees must receive regular training on cybersecurity practices, such as the safe use of work email, how to handle customer data, and ethical principles in maintaining information confidentiality. With a strong organisational culture in terms of cybersecurity, internal threats such as *insider threats* can be minimised (Elitery, 2024) .

Overall, strategies for protecting personal data in the digital age must be holistic, adaptive, and sustainable. No single technology or policy can fully protect data. Efforts must involve layers of protection ranging from individuals to companies to

governments in order to deal with increasingly sophisticated threats. With a combination of technology, regulation, digital literacy, and a strong security culture, personal data can be better protected from various cyberattack risks.

## Conclusion

Cyber security threats in the digital age are becoming increasingly complex and diverse, ranging from phishing, malware, ransomware, to attacks on Internet of Things devices and the use of *deepfake* technology. These threats not only endanger individuals with the risk of personal data theft, but also have a broader impact on economic and social stability, as well as national security. This complexity emphasises that cyber security is no longer merely a technical issue, but a strategic problem that involves various dimensions of modern life.

In facing these challenges, personal data protection strategies must be comprehensive and multi-layered. These efforts include the use of security technologies such as encryption, two-factor authentication, and artificial intelligence-based monitoring, supported by clear regulations through the implementation of the Personal Data Protection Act and international cooperation. In addition, digital literacy among the public plays an important role in making individuals more aware of social manipulation and unsafe data sharing practices.

By combining advanced technology, strong legal policies, and a culture of digital awareness, the protection of personal data can be significantly improved. Data protection is not only the responsibility of the government or digital service providers, but a shared responsibility that involves every individual. Only through cross-sector collaboration can society safely utilise digital technology, while minimising the risk of cyber threats that continue to evolve in the future.

## References


A. Yusliwidaka. (2024). *A Discourse of Personal Data Protection: How Indonesia Responsible under Domestic and International Law?* https://journal.unnes.ac.id/journals/pandecta/article/view/13279

Abdullah Azizi, Mohammad Qias Mohammadi, Abdul Wahid Samadzai, & Abdul Qayum Shafaq. (2025). *AI IN CYBER DEFENSE: PRIVACY RISKS, PUBLIC TRUST, AND POLICY CHALLENGES*. https://journal.undiknas.ac.id/index.php/fisip/article/view/6278

AF Sadeli. (2023). *Awareness of Personal Data Protection Law in Concern to Scientific Research*. https://jurnal.unpad.ac.id/jkip/article/view/47526

Aleksandra Kuzior, Inna Tiutiunyk, Anetta Zielińska, & Roland Kelemen. (2024a). *Cybersecurity and cybercrime: Current trends and threats*. https://jois.eu/files/12_1441_JIS_Tiutiunyk%20et%20al.pdf

Aleksandra Kuzior, Inna Tiutiunyk, Anetta Zielińska, & Roland Kelemen. (2024b). *Cybersecurity and cybercrime: Current trends and threats*. https://jois.eu/files/12_1441_JIS_Tiutiunyk%20et%20al.pdf

Ana Sofa Yuking. (2018). *Personal Data Protection in Indonesia: Legal Perspective*. https://ijmmu.com/index.php/ijmmu/article/view/1773

B. Dupont. (2022). *Cyber resilience revisited: Law and international relations*.

Bolderston, A. (2008). Writing an Effective Literature Review. *Journal of Medical Imaging and Radiation Sciences*, 71–76.

Csirt BPIIP. (2025). *Ancaman Siber 2025: Indonesia Harus Waspada AI Agentik*. https://csirt.bpip.go.id/posts/ancaman-siber-2025-indonesia-harus-waspada-ai-agentik

D. Febriawan. (2024). *Understanding Indonesia's Cyber Security Policies and Strategies*.

Diskominfo Sukoharjo. (2025). *Tips Melindungi Data Pribadi*. https://diskominfo.sukoharjokab.go.id/berita/tips-melindungi-data-pribadi-1

Dudy Heryadi, Robby Rizaldi, Tia Panca Rahmadhani, Feby Diah Miranti, & Febyanti Juliastica. (2024). *Indonesia's Role as A Cyber Protector in Southeast Asia*. https://jurnal.idu.ac.id/index.php/DefenseJournal/article/view/13097

Elitery. (2024). *Keamanan Siber dalam UU Perlindungan Data Pribadi*. https://elitery.com/articles/penerapan-keamanan-siber-dalam-menunjang-uu-perlindungan-data-pribadi/

Eliyah, E., & Aslan, A. (2025). STAKE'S EVALUATION MODEL: METODE PENELITIAN. *Prosiding Seminar Nasional Indonesia*, *3*(2), Article 2.

F. Cremer. (2022). *Cyber risk and cybersecurity: A systematic review of data availability*. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8853293/

F. Rafiq. (2022). *Privacy Prevention of Big Data Applications: A Systematic Review*.

Graduate BINUS University. (2024). *7 Jenis Ancaman Cybersecurity terhadap Keamanan Data*. https://graduate.binus.ac.id/2024/02/07/7-jenis-ancaman-cybersecurity-terhadap-keamanan-data/

H. Maliha. (2024). *Cybersecurity and Fintech Studies in Academic Discussion*.

J. Järveläinen. (2025). *Towards a framework for improving cyber incident reporting*.

Karier.mu. (2024). *Cara Melindungi Informasi Pribadi di Era Digital*. https://www.karier.mu/blog/umum/cara-melindungi-informasi-pribadi-di-era-digital/

ME Susila. (2024). *Cyber Espionage Policy and Regulation*. https://journal.unpad.ac.id/pjih/vol11/iss1/2/

MF Adhiwisaksana. (2023). *Personal Data Protection with Foreign Element as Private International Law Issue*.

MF Asyrofi. (2025). *Cybersecurity Of Work From Anywhere Model For Government*.

Naeem AllahRakha. (2024). *Cybersecurity Regulations for Protection and Safeguarding Digital Assets (Data) in Today's Worlds*. https://journal.unnes.ac.id/journals/lslr/article/view/2081

Najamuddin Gani. (2024). *Legal Politics and Data Protection in Indonesia: A Case Study of the National Data Center Hacking*. https://fhukum.unpatti.ac.id/jurnal/sasi/article/view/2213

P. Swire. (2024). *Risks to cybersecurity from data localization, organized by jurisdiction*.

R. Anggriawan. (2022). *Passenger Name Record Data Protection under European Regulations*.

R. Ayunda. (2023). *Personal Data Protection to E-Commerce Consumer: Challenges and Legal Certainty*.

R. Ducato. (2020). *Data protection, scientific research, and the role of information*.

Reno Andre Permana. (2025). Analisis Metode dan Teknologi untuk Perlindungan Data dan Informasi dari Ancaman Siber. *Jurnal MENTARI Manajemen, Pendidikan Dan Teknologi Informasi*, *3*(2). https://journal.pandawan.id/mentari/article/view/744

S. Busetti. (2025). *Evaluating incident reporting in cybersecurity: Theory-based evaluation*.

S. Slapničar. (2022). *Effectiveness of cybersecurity audit*.

S. Watini. (2024). *Cybersecurity in Learning Systems: Data protection and security concerns*.

ST Hossain. (2025). *Cybersecurity in local governments: A systematic review and framework of key challenges*.

T. Daim. (2024). *Monitoring cybersecurity technology through the years*.

Titis Pandan Wangi Reformasi & Hasrul Buamona. (2024). *Cybersecurity Law Exploration: Personal Data Protection in 2023*. https://journal.formosapublisher.org/index.php/jlca/article/view/10376

W. S. Admass. (2024a). *Cyber security: State of the art, challenges and future directions*.

W. S. Admass. (2024b). *Cybersecurity: State of the art, challenges and future directions*.