Security and Privacy in the Digital Era: Overcoming Challenges and Enhancing Protection

I Wayan Sindia Griya Danika[1]
[1]Institut Agama Hindu Negeri Tampung Penyang Palangka Raya
[1]dana.danikadas@gmail.com

ABSTRACT

The advancing information technology has provided users in the digital era with faster and easier access to information. However, this progress also brings forth new challenges in terms of information security and privacy. Cybercrime, hacking, and identity theft are some of the threats that need to be addressed in order to uphold the security and privacy of information. This article discusses the challenges and threats in information security and privacy in the digital era and provides strategies for enhancing protection. The strategies discussed include the implementation of data encryption, the use of strong passwords, and stringent data access management. Additionally, it is important for users and organizations to understand these risks and threats and take action to safeguard their information security and privacy. By following the guidelines and strategies outlined in this article, it is hoped that users and organizations can remain safe and protected in their use of information technology. Furthermore, awareness and appropriate actions can also help improve overall information security and privacy in the digital era.

Keywords: Security, Privacy, Digital Era

I. Introduction

In this digital era, access to information has become easier and faster, thanks to advances in information technology such as the internet and mobile devices (Safdar et al., 2017). However, the benefits gained from information technology are also balanced with new challenges, especially in terms of security and privacy. Along with the increasing access and use of information technology, there is also an increase in risks and threats to information security and privacy. Some of the challenges faced in terms of information security and privacy in the digital era include cybercrime, hacking, identity theft, and unauthorized surveillance (Tyagi et al., 2020).

Security and privacy are two very important things in the digital era (Babun et al., 2021). As technology advances, people are increasingly relying on digital

devices to perform various activities, including accessing information, conducting transactions, communicating, and so on. This raises new challenges in maintaining data security and privacy because more sensitive information is stored and transmitted through digital devices(Hatzivasilis et al., 2019). One of the biggest challenges in digital security and privacy is cybercrime. Cybercrime can occur in various forms such as hacking, viruses, phishing, and so on. To overcome this challenge, many security technologies and solutions have been developed such as data encryption, intrusion detection systems, and firewalls. However, not all digital device users have sufficient knowledge and skills to properly implement these security solutions(Roman et al., 2013).

In addition, privacy is also becoming an increasingly complex issue. In the digital era, a lot of data is collected by companies and organizations for various purposes, such as market analysis, product personalization, and targeted advertising. This data can contain sensitive information about users, such as location, preferences, and even medical history. Therefore, privacy protection is very important to protect individual rights(Rui & Yan, 2019).

To overcome security and privacy challenges in the digital era, cooperation between users, organizations, and governments is needed. Users should be more careful in using digital devices and take steps to improve their own security and privacy, such as using strong passwords and avoiding sharing sensitive information online. Organizations must improve their data security and privacy, including conducting employee training, implementing appropriate security solutions, and responding quickly to security breaches. Governments also have an important role in providing the necessary regulations and security standards to protect user security and privacy. Security and privacy in the digital era are complex challenges but also important to overcome(Suo et al., 2012). The more people and organizations that realize the importance of security and privacy, the better for society as a whole. Therefore, everyone and every organization needs to pay attention to security and privacy in their use of digital devices.

Security and privacy in the digital era are increasingly complex issues that are of concern to many parties. In the digital era, a lot of personal and sensitive information is transmitted through the internet and stored on digital devices such

as mobile phones, computers, and IoT (Internet of Things) devices. This information can include financial information, medical information, location information, and other personal information (Jhanjhi et al., 2021). If this information falls into the wrong hands, it can endanger user privacy and security. Digital security is very important to prevent cybercrime and unauthorized use of sensitive information. Cybercrime can take the form of website hacking, virus attacks, phishing, and more. One solution to overcome this challenge is to use security solutions such as data encryption, firewalls, and intrusion detection systems. However, these solutions are not enough to provide optimal security because cybercrime is becoming more complex and sophisticated. Therefore, companies and organizations must continue to develop and improve their security technology, as well as conduct training and education for employees and users to increase security awareness(Alzoubi et al., 2021).

To overcome security and privacy challenges in the digital era, there are several things that can be done. First, users should be more careful in using digital devices and take steps to improve their own security and privacy. Users should use strong passwords, avoid sharing sensitive information online, and activate security features on their devices. Second, organizations must improve their data security and privacy, including conducting employee training, implementing appropriate security solutions, and responding quickly to security breaches. Finally, governments also have an important role in providing the necessary regulations and security standards to protect user security and privacy(Alrawais et al., 2017). Security and privacy in the digital era are important issues that deserve serious attention. All parties, whether users, organizations, or governments, must work together to overcome these security and privacy challenges. By increasing security and privacy awareness and taking appropriate action, we can improve our data protection and prevent cybercrime and misuse of our personal data in the digital era. In addition, users should understand their rights in terms of privacy and ask for explanations from companies or organizations that collect their data about how that data will be used.

Meanwhile, governments also have an important role in protecting user security and privacy in the digital era. Governments must create effective

regulations and security standards to protect user security and privacy. They must also strengthen penalties for cybercriminals and increase international cooperation to combat cross-border cybercrime. In an increasingly digitalized era, security and privacy are becoming increasingly important issues. Many people upload their personal information to the internet, such as social media accounts, emails, or websites, and without adequate security, this information can easily be stolen by irresponsible individuals. However, it is not only that, security and privacy are also related to human rights, including the right to privacy and freedom of expression(Kshetri, 2017).

Technology solutions, such as encryption and network security, have been developed. However, technology solutions alone are not sufficient. Local wisdom can contribute to enhancing security and privacy in the digital era. Local wisdom encompasses the local knowledge and practices acquired through experience and passed down through generations. It can assist communities in adopting wiser and more cautious approaches when interacting with digital technology, thereby preventing misuse and privacy breaches. Therefore, research on security and privacy in the digital era should incorporate the concept of local wisdom as a factor that can help address challenges and enhance protection. By understanding the local wisdom associated with digital technology, communities can gain better insights into using technology safely and wisely, and develop more effective solutions to tackle security and privacy issues. For instance, local wisdom may involve practices such as employing strong and complex passwords, refraining from uploading excessively detailed or sensitive personal information online, and limiting access to social media or email accounts. Moreover, concepts like privacy rights and freedom of expression can be explored and strengthened within the context of local wisdom, enabling communities to better comprehend and value these principles in the digital era(Yang et al., 2020).

It is crucial for information technology users to comprehend these risks and threats and take measures to safeguard their information security and privacy. Likewise, companies and organizations must prioritize security and privacy when managing their data and information systems. This article aims to discuss the challenges and threats related to information security and privacy in the digital

era, while also providing guidance and strategies to enhance protection and address these challenges. It is hoped that this article will assist individuals and organizations in maintaining a secure and protected environment while utilizing information technology(Abomhara & Koien, 2014).

II. Discussion

A. The Definition of Digital Security and Privacy

Digital security refers to the measures taken to protect computer systems, networks, and data from unauthorized access, unauthorized use, unauthorized alteration, or damage. This involves implementing security measures such as using strong passwords, data encryption, regular software updates, and utilizing firewalls to prevent unauthorized access. Digital privacy, on the other hand, relates to the protection of individuals' personal information in the digital environment. It encompasses control and oversight over the collection, use, and disclosure of personal information by others. Digital privacy involves policies and practices designed to maintain the confidentiality and security of personal information, as well as provide individuals with rights and control over their personal data(Khan et al., 2020).

In the digital era, digital security and privacy have become increasingly important due to the growing amount of personal data stored and exchanged electronically. Threats such as hacking, identity theft, and malware attacks are becoming more complex and frequent. Therefore, it is crucial to understand and implement proper digital security and privacy practices to safeguard the confidentiality, integrity, and availability of personal information. In the context of digital security, several key elements are important to be understood:

1. Authentication: The process of verifying the identity of a user or system. This involves the use of unique combinations such as usernames and passwords, as well as other authentication methods like fingerprint scanning or two-factor authentication.
2. Encryption: The process of transforming data into a form that is unreadable or unintelligible, except by those who possess the

appropriate encryption key. Encryption is used to protect data when it is transmitted over a network or stored on a device.

3. Network Security: Involves measures to protect computer networks from external threats such as malware attacks, Distributed Denial of Service (DDoS) attacks, and hacking attempts.
4. Access Management: The implementation of policies and controls to ensure that only authorized users have access to specific digital resources. This includes the use of access rights, permissions, and data privacy controls.
5. Software Security: Involves the implementation of secure software development practices, including ensuring ongoing software updates, validating user inputs, and eliminating vulnerabilities that can be exploited by hackers.

Meanwhile, in the context of digital privacy, several important aspects include:

1. Data Collection: Ensuring that personal information is collected lawfully and in accordance with regulations, and providing transparency to individuals regarding the purpose and types of data being collected.
2. Data Storage: Taking security measures to protect personal data from unauthorized access, such as using encryption and appropriate physical security settings.
3. Data Usage: Ensuring that personal data is only used for agreed-upon purposes and providing options for individuals to give consent or restrict the use of their data.
4. Data Disclosure: Providing clarity on who can receive personal data and under what circumstances the data may be disclosed to third parties.
5. Individual Rights: Granting individuals the rights to access, correct, delete, or restrict the use of their personal data, as well as empowering them to control their own privacy.

In the increasingly complex and interconnected digital era, it is important for organizations and individuals to understand, implement, and comply with appropriate digital security and privacy practices to protect data and maintain privacy.

B. The importance of digital security and privacy

Digital security and privacy have significant importance in the current digital era. Here are several reasons why digital security and privacy are crucial (Sivaraman et al., 2015):

1. Protection of Personal Data: Digital security and privacy involve measures to protect individuals' personal data from unauthorized access, unauthorized use, and misuse. Personal data such as identity information, financial information, and medical information need to be safeguarded to prevent them from falling into the wrong hands or being used in harmful ways.
2. Preventing Cybercrime: Cybercrimes such as hacking, malware attacks, and identity theft are on the rise in the digital era. By implementing strong digital security measures, it is possible to prevent attacks that can harm individuals, businesses, and institutions.
3. User Trust: Strong security and privacy are crucial factors in building user trust in digital services and the companies that provide them. Users who trust are more likely to use digital services, share information, and transact online.
4. Regulatory Compliance: Many countries have implemented laws and regulations related to data security and privacy, such as the GDPR in the European Union and the Personal Data Protection Act in several countries. Having good digital security and privacy helps ensure that organizations comply with applicable legal requirements.
5. Business Security and Reputation: Weak digital security can jeopardize business and company reputation. Data security breaches that result in the leakage of personal information can damage a company's image and lead to the loss of trust from customers and business partners.
6. Protection against Cyberbullying and Cyberharassment: Digital security and privacy also play a role in protecting individuals from threats such as cyberbullying, cyberharassment, and other forms of online abuse. Having control and good protection over online privacy can help prevent and address such cases.

7. System and Infrastructure Security: Good digital security also involves protecting vital systems and digital infrastructure, such as computer networks, hardware, and software. Threats to security can cause serious operational disruptions and have negative impacts on various sectors, including businesses, governments, and critical infrastructure.
8. Protection of Freedom and Human Rights: Digital security and privacy are closely related to the protection of freedom and human rights. In an era where personal data is highly valuable, it is important to ensure that individuals have full control over their personal information. By implementing good security and privacy measures, we can protect individuals' rights to communicate, express themselves, and maintain their digital identities.
9. Protecting Business Confidentiality: Digital security and privacy are also important in safeguarding business confidentiality, including trade secrets, strategic information, and intellectual property. Security breaches can result in data theft and business information leaks that can harm competition and company reputation.
10. Enhancing Transaction and E-commerce Security: Strong digital security and privacy also play a crucial role in enhancing trust in online transactions and e-commerce. With effective security measures in place, individuals can feel more secure when shopping online, conducting financial transactions, and participating in the digital economy.
11. Innovation and Technological Advancement: Good digital security and privacy enable further innovation and technological advancement. By having confidence in data security and privacy, individuals and organizations are more likely to adopt new technologies and participate in the evolving digital ecosystem.
12. Addressing Cyber Threats: In an increasingly interconnected world, cyber threats have become more complex and serious. Strong digital security and privacy aid in the handling and mitigation of cyber attacks, protecting critical infrastructure, and ensuring stability and security in the digital environment.

In order to maximize the benefits and address the challenges in the digital era, it is important to give serious attention to digital security and privacy. By implementing the right policies, technologies, and practices, we can safeguard data security, protect individual privacy, and create a secure, reliable, and responsible digital ecosystem(Weber, 2010). By understanding the importance of digital security and privacy, individuals, organizations, and governments can collaborate to protect data and preserve privacy in this rapidly evolving digital age.

C. Threats to digital security and privacy

Digital security and privacy are faced with various threats that need to be aware of. Here are some common threats to digital security and privacy (Sicari et al., 2015):

1. Malware Attacks: Malware refers to malicious software designed to disrupt systems, steal information, or interfere with normal computer or network operations. Examples include viruses, worms, trojans, ransomware, and spyware.
2. Hacking Attacks: Hackers use various methods and techniques to gain unauthorized access to computer systems or networks. They can steal data, damage systems, or control them for their own purposes.
3. Distributed Denial of Service (DDoS) Attacks: DDoS attacks aim to make system resources unavailable by overwhelming the target system with excessive network traffic. This results in service disruptions and operational disturbances.
4. Identity Theft: Identity theft involves acquiring and using someone's personal information without permission to engage in criminal activities, financial fraud, or misuse of identity in a digital context.
5. Phishing: Phishing is an attempt to obtain sensitive information such as passwords, credit card numbers, or financial information by disguising as a trustworthy entity through emails, instant messages, or fake websites.
6. Data Breaches: Data breaches occur when personal information is accessed, stolen, or disclosed by unauthorized parties. This can result in financial loss, identity theft, or misuse of personal information.

7. Software and System Vulnerabilities: Software and systems that are not regularly updated or have security vulnerabilities can be exploited by hackers to gain unauthorized access or control over the system.
8. Misuse of Data by Authorized Parties: Individuals or entities with legitimate access to data, such as company employees or service providers, can misuse that information for personal gain or violate individual privacy.
9. Mobile Data Theft: The increasing use of mobile devices and mobile applications also raises the risk of data theft through attacks on apps, insecure public Wi-Fi, or the hacking of lost or stolen devices.
10. Social Threats: Social threats involve manipulative practices or scams targeted at individuals through social techniques, such as social engineering or identity forgery, to obtain sensitive information.

It is important to be aware of these threats and take steps to protect our digital security and privacy. Using up-to-date security software, practicing recommended security measures, following good security practices, and increasing awareness of existing risks are important steps to maintain our digital security and privacy(Hassan et al., 2020). Additionally, collaboration among individuals, organizations, and governments is key in addressing digital security and privacy challenges. Sharing information, developing strict policies and regulations, and collaborative efforts to identify and address emerging threats can help create a safer and protected digital ecosystem.

D. Improving Digital Security and Privacy Protection

To enhance digital security and privacy protection, the following are some steps that can be taken (Ziegeldorf et al., 2014):

1. Use Strong Passwords: Use strong and unique passwords for your online accounts. Combine uppercase and lowercase letters, numbers, and symbols to enhance password security. Avoid using easily guessable passwords or ones that have been used for multiple accounts.
2. Enable Two-Factor Authentication: Enable two-factor authentication (2FA) on accounts that support it. This provides an additional layer of security by requiring verification through another device, such as a code sent via SMS or an authentication app.

3. Regularly Update Software: Ensure that your operating system, antivirus software, and other applications are always up to date with the latest versions. These updates often contain security patches to address discovered vulnerabilities.
4. Use Secure Internet Connections: When connecting to the internet, make sure to use a secure and encrypted connection. Avoid using insecure public Wi-Fi networks, especially for financial transactions or accessing sensitive information.
5. Beware of Phishing: Be cautious of phishing attempts that may trick you into disclosing personal information or clicking on malicious links. Verify the source before providing sensitive information or clicking on suspicious links.
6. Manage App Permissions: Check and carefully manage app permissions. Ensure that apps only have the necessary access to function and do not collect more personal data than required.
7. Encrypt Data: Use encryption for sensitive data, both on your devices and when transferring it over networks. Encryption can help protect data from unauthorized access and safeguard your privacy.
8. Secure Mobile Devices: Enable screen locking with a PIN or fingerprint on your mobile devices. Additionally, consider using mobile security software and avoid downloading apps from untrusted sources.
9. Monitor Your Digital Footprint: Be aware of what you share online and manage your digital footprint. Limit the personal information you share on social media platforms and avoid posting information that can provide clues about your whereabouts, schedule, or activities.
10. Enhance Digital Security Awareness: Continuously improve your knowledge and awareness of good digital security practices. Follow reliable sources, stay updated on security threats, and share knowledge with those around you.
11. By adopting the above steps, you can enhance your digital security and privacy protection. However, it's also important to consider the following:

12. Manage Personal Data Wisely: Consider what personal data you provide to online platforms and applications. Read privacy policies carefully and understand how your data will be used and protected.
13. Use Secure Cloud Security Services: If you store sensitive data in the cloud, make sure to use secure and trusted services. A reputable cloud provider will offer additional security layers such as encryption and restricted access.
14. Regularly Backup Data: Always back up your important data. By having secure data copies, you can reduce the risk of data loss due to malware attacks, hardware failures, or natural disasters.
15. Use a Virtual Private Network (VPN): If you frequently connect to public networks or want to enhance your privacy while browsing, consider using a VPN. A VPN can hide your online activities and encrypt your data when connected to the internet.
16. Maintain Physical Device Security: Properly secure your physical devices. Ensure that your mobile devices, laptops, or computers are not easily accessible to unauthorized individuals.
17. Follow Digital Security Principles in the Workplace: If you work with sensitive data in the workplace, make sure to comply with company security policies. This includes using strong passwords, securely utilizing resources, and reporting suspicious security incidents.
18. Engage in Digital Security Education and Training: Enhance your understanding of digital security and privacy by continuously updating your knowledge through education and training. There are numerous online resources available to help you learn better digital security practices.

By adopting these measures, you can significantly enhance your digital security and privacy protection. It is important to remember that digital security is an ongoing effort that requires awareness, caution, and compliance with relevant best practices in line with technological advancements.

III. Closing

In the increasingly advanced digital era, digital security and privacy have become crucial aspects. Threats to digital security and privacy are becoming more complex and can have serious implications for individuals, companies, and society as a whole. Therefore, it is important to address these challenges and enhance protection for digital security and privacy. This research highlights the significance of digital security and privacy in the rapidly evolving digital era. The escalating threats to digital security and privacy necessitate serious efforts to counter these challenges and strengthen protection. Literature review serves as an effective approach in understanding the issues of digital security and privacy. In relation to the local wisdom of the Kalimantan tribe, there is potential for integrating local values and practices to enhance digital security and privacy. This can result in better and more contextually relevant solutions that cater to local needs. To improve the protection of digital security and privacy, several steps can be taken, such as using strong passwords, enabling two-factor authentication, regularly updating software, and utilizing secure internet connections. Furthermore, it is essential to enhance awareness and education on digital security, foster collaboration among various stakeholders, enforce strict regulations, and actively involve the community. By adopting these measures and incorporating local wisdom, it is anticipated that holistic protection of digital security and privacy can be achieved. Strong digital security and privacy not only safeguard individuals and organizations but also provide a solid foundation for the development of technology and sustainable digital growth.

However, it is important to remember that digital security and privacy require ongoing efforts. Threats to them continue to evolve alongside technological advancements. Therefore, it is crucial to continuously monitor and evaluate digital security practices, as well as adopt innovative and adaptive solutions to address emerging challenges. By doing so, we can ensure that the digital era can provide maximum benefits while maintaining optimal security and privacy. This research has highlighted the importance of digital security and privacy, as well as the potential threats that can impact both aspects.

Bibliography

Abomhara, M., & Koien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. *2014 International Conference on Privacy and Security in Mobile Systems, PRISMS 2014 - Co-Located with Global Wireless Summit*, *May*, 1–8. https://doi.org/10.1109/PRISMS.2014.6970594

Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog Computing for the Internet of Things: Security and Privacy Issues. *IEEE Internet Computing*, *21*(2), 34–42. https://doi.org/10.1109/MIC.2017.37

Alzoubi, Y. I., Al-Ahmad, A., & Jaradat, A. (2021). Fog computing security and privacy issues, open challenges, and blockchain solution: An overview. *International Journal of Electrical and Computer Engineering*, *11*(6), 5081–5088. https://doi.org/10.11591/ijece.v11i6.pp5081-5088

Babun, L., Denney, K., Celik, Z. B., McDaniel, P., & Uluagac, A. S. (2021). Una encuesta sobre plataformas IoT: perspectivas de comunicación, seguridad y privacidad. *Computer Networks*, *192*, 108040. https://doi.org/10.1016/j.comnet.2021.108040

Hassan, M. U., Rehmani, M. H., & Chen, J. (2020). Differential Privacy Techniques for Cyber Physical Systems: A Survey. *IEEE Communications Surveys and Tutorials*, *22*(1), 746–789. https://doi.org/10.1109/COMST.2019.2944748

Hatzivasilis, G., Soultatos, O., Ioannidis, S., Verikoukis, C., Demetriou, G., & Tsatsoulis, C. (2019). Review of security and privacy for the internet of medical things (IoMT): Resolving the protection concerns for the novel circular economy bioinformatics. *Proceedings - 15th Annual International Conference on Distributed Computing in Sensor Systems, DCOSS 2019*, *May 2019*, 457–464. https://doi.org/10.1109/DCOSS.2019.00091

Jhanjhi, N. Z., Humayun, M., & Almuayqil, S. N. (2021). Cyber security and privacy issues in industrial internet of things. *Computer Systems Science and Engineering*, *37*(3), 361–380. https://doi.org/10.32604/CSSE.2021.015206

Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2020). A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. *IEEE Communications Surveys and Tutorials*, *22*(1), 196–248. https://doi.org/10.1109/COMST.2019.2933899

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, *41*(10), 1027–1038. https://doi.org/10.1016/j.telpol.2017.09.003

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

Rui, Z., & Yan, Z. (2019). A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification. *IEEE Access*, *7*, 5994–6009. https://doi.org/10.1109/ACCESS.2018.2889996

Safdar, Z., Farid, S., Pasha, M., & Safdar, K. (2017). A Security Model for IoT based Systems. *Technical Journal, University of Engineering and Technology (UET)*, *22*(4), 74–84.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of things: The road ahead. *Computer Networks*, *76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., & Mehani, O. (2015). Network-level security and privacy control for smart-home IoT devices. *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob 2015*, *June 2016*, 163–167. https://doi.org/10.1109/WiMOB.2015.7347956

Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the internet of things: A review. *Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012*, *3*(March), 648–651. https://doi.org/10.1109/ICCSEE.2012.373

Tyagi, A. K., Nair, M. M., Niladhuri, S., & Abraham, A. (2020). Security , Privacy Research issues in Various Computing Platforms : A Survey and the Road Ahead. *Journal of Information …*, *15*, 1–16. http://search.ebscohost.com/login.aspx?direct=true%5C&profile=ehost%5C&scope=site%5C&authtype=crawler%5C&jrnl=15541010%5C&AN=143489195%5C&h=45masT0R7A%2FLouGuAarLEFN9oPJH9WIjXTg%2FEnWT8cvxzXAHxr7X28emfKR8%2FkJdwIOFAsBqXhQYEXTTRGsHng%3D%3D%5C&crl=c

Weber, R. H. (2010). Internet of Things - New security and privacy challenges. *Computer Law and Security Review*, *26*(1), 23–30. https://doi.org/10.1016/j.clsr.2009.11.008

Yang, P., Xiong, N., & Ren, J. (2020). Data Security and Privacy Protection for Cloud Storage: A Survey. *IEEE Access*, *8*, 131723–131740. https://doi.org/10.1109/ACCESS.2020.3009876

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the internet of things: Threats and challenges. *Security and Communication Networks*, *7*(12), 2728–2742. https://doi.org/10.1002/sec.795