Berkala Ilmu Perpustakaan dan Informasi, Vol. 17, No. 2, Desember 2021, Hal. 238-249
https://doi.org/10.22146/bip.v17i1.2082
ISSN 1693-7740 (Print), ISSN 2477-0361 (Online)
Tersedia online di https://journal.ugm.ac.id/v3/BIP

Examining cyber security implementation through TLS/SSL on academic institutional repository in Indonesia

Irhamni Ali
Department of Information Science, University of North Texas
3940 North Elm, Suite E292 Denton , Texas 76203
e-mail: fnuirhamni@my.unt.edu

Naskah diterima: 1 Juli 2021, direvisi: 23 September 2021, disetujui: 21 Oktober 2021

ABSTRAK

Pendahuluan. Tulisan ini mengkaji keamanan siber AIR di Indonesia dengan menganalisis aspek keamanan yang berfokus pada protokol keamanan jaringan SSL (*Secure Socket Layer*) yang berfungsi mengamankan komunikasi, dan teknologi SSL terbaru yang disebut TLS (*Transport Layer Security*)..
Metode penelitian. Penelitian ini dilakukan melalui eksperimen pada AIR terbaik di Indonesia di perguruan tinggi swasta dan negeri..
Data analisis. Data dianalisis secara deskriptif dengan menggunakan metode *scoring SSL Scoring*.
Hasil dan Pembahasan. Temuan serius adalah bahwa sebagian besar Repositori Institusi Akademik Indonesia memiliki masalah keamanan yang rentan di TLS/SSL mereka dan dapat menyebabkan masalah yang merusak keamanan aset informasi mereka.
Kesimpulan dan Saran. Berdasarkan temuan tersebut, AIR Indonesia mendesak untuk menerapkan intervensi keamanan bagi AIR untuk memperbarui teknologi dan kebijakan untuk melindungi aset informasi..

Kata kunci: keamanan cyber; keamanan repositori kelembagaan akademik; keamanan perpustakaan digital

ABSTRACT

Introduction. *This paper examines the cybersecurity of AIR in Indonesia by analyzing the security aspect focusing on the security protocols involving network called TLS (Transport Layer Security) and SSL (Secure Socket Layer), which has functions to secure the communication.*
Data Collection Methods. *This research was conducted through experimental on the best AIR in Indonesia at private and public universities.*
Data Analysis*. The data were descriptively analysed using scoring method of SSL Scoring.*
Results and Discussion. *Several issues found was most Indonesian Academic Institutional Repositories have vulnerable security issues in their TLS/SSL and could cause problems disastrous for their information asset's security.*
Conclusion. *Based on the findings, Indonesian AIR is urgent to implement security intervention for AIR to update the technology and policy to protect the information asset.*

Keywords: *cyber security; academic institutional repository security; digital library security*

A. INTRODUCTION

The implementation of the Academic Institutional Repository (AIR) has become a prominent topic for librarians. The idea of AIR has provided an easier way to collect, preserve, and disseminate research output at universities and research institutions (Zervas et al., 2019). The AIR concept has developed new beehives to access the AIR content and become a trusted place to keep the data in their space. AIR impacted on how the higher education business process and turns it into the Resources Center of Knowledge. Based on the National Library of Indonesia's data in 2020, more than 7890 academic IR is currently in Indonesia (Perpusnas, 2020). Nature magazine in 2019 declares Indonesia is one of the promising tops open-access publishing charts, particularly in AIR (Noorden, 2019). Cybersecurity is a complicated entity which involves several issues, and cyber security's first issue is to to ensure all of their information assets can be appropriately secured.

Cybersecurity in AIR involves many aspects, it is not all about threat access to the hardware; it also discusses to securing all software, including assets like personal data, content, and other crucial data produced from AIR from an unwanted incident that can corrupt the reputation university. Cybersecurity is all about safety and security, and strengthening an ecosystem is to understand, analyze, and manage the cyber risks that it faces with the design of a security architecture that includes appropriate cybersecurity controls that will mitigate the risks (Kavallieratos & Katsikas, 2020). There are 50% of reviewed European digital repositories (listed in OpenDOAR.org registry) that discuss the library and information science field does not use any kind of transfer security for access and other user data (Formanek & Zaborsky, 2017a). Many higher education institutions in Indonesia adopt open source as their primary platform for their AIR operational system (Liauw & Genoni, 2017a). However, there is never any evaluation in the security aspect of the AIR system, particularly in the cybersecurity aspect.

This paper investigates the cybersecurity of AIR in Indonesia by analyzing the security aspect focusing on the security network protocols TLS (Transport Layer Security) and SSL (Secure Socket Layer), which has functions to secure the communication between client and server. TLS/SSL work with encrypted connection between a client (e.g., a browser) and a server. This research will reveal how secure the relationship between the AIR, the potential risks that could happen and also what solutions to AIR administrators in Indonesia to ensure the safety of AIR data and user data. Using experimental test in order give empirical evidence on the real cyber security implementation data is AIR in Indonesia. The paper concludes there should be another cybersecurity interference on the AIR in Indonesia.

B. LITERATURE REVIEW

Indonesian Academic Institutional Repository

Indonesia is a fast growing country that currently has 100 state higher education institutions and 2,972 private higher education institutions and serving a population of 255 million people in 2015 (Kemristekdikti, 2020). In these several years, Indonesian Higher Academic Institutional Repository has transformed into digital repository and contribute a significant engagement to the latest research access in the academic world. As a promising country on Open Access, Indonesia has 20,000 journal articles published in 2017 with 81% contribute from Indonesia-affiliated author and available to read for free somewhere online, and approximately 74% are published with open-access licenses, meaning they could be legally redistributed (Noorden, 2019). Some institutions are Binus University, Bogor Agricultural University, Graduate Program of Management and Business Bogor Agricultural University, Borneo University, Bunda Mulia University,CISRAL Universitas Padjadjaran, Diponegoro University (UNDIP), EEPIS, Gunadarma University, Hasanuddin University. The IPB Repository (Bogor Agricultural University Repository) is one of the biggest

open access institutional repositories in Indonesia maintained by Bogor Agricultural University with 61274 items that stores and provides access to articles; theses; unpublished; books (Mita Paul & Anindya Basu, 2015). Indonesia is a new country that become promising growth with IR implementation.

The high rise of the Indonesian academic institutional repository was based on establishing several legal formal and ministry order decrees to create the academic institutional repository. Some legal formalities are the Ministry of National Education Act No. 17 / 2010, which mandates the use of IRs to "upload electronically all scholarly works by students/lecturers/ researchers/staff of any higher education institution" and In 2011, Indonesian Higher Education Directorate operationalized. The Act also issuing Circular 2050/E/T/2011, "Kebijakan Unggah Karya Ilmiah dan Jurnal" or Policies on the Uploading of Scholarly Works and Journals (Liauw & Genoni, 2017a). The current developments and the establishment of various policies regarding AIR indicate Indonesia will have significant increase in exposure to Indonesian research and publishing.

Cyber Security Issue on Academic Institutional Repository

Cyber Security has become an important issue since the advancement of the internet and data communication across the world; in higher education, cybersecurity is not about theory but also implementation entity (Agrawal & Jain, 2018). Thus, cybersecurity is a critical topic, particularly in the AIR, that contains various data and tends to have great potential to become the victim of cyber threats. Cyber threat has become a complicated entity since it not only involves natural causes but also involving complex algorithms. However, most cyber threats are trying to cripple all services (Humayun et al., 2020a). One of the examples of cybersecurity threats is the DoS (Denial of Service) attacks when the AIR is intentionally overloaded with so many requests that the service cannot respond, and the access is stopped even for authorized users (Kovářová, 2011; Radivilova et al., 2018). Cybersecurity is a serious issue to protect the accountability of AIR and the university.

Cybersecurity has been a significant issue since involving many components of aspect of policy. There has been a lack of attention about the repository's security, which causes their understanding of the repository was not strong enough (Priyanto & Miksa, 2015). Cybersecurity's primary goal is to create a mechanism to protect individuals and organizations' assets from unauthorized access and uses (Humayun et al., 2020b). The problem also came from the local and non-standard practices in AIR management on the policy in the security regarding the sensitive information appeal in the AIR content that reveals private, confidential, and copyright issues in an AIR content (Liauw & Genoni, 2017b). Cybersecurity is about keeping information safe physically and keeping information securely held, access using tools and policy. There should be a significant concern to AIR administrators in Indonesia that still needs to be addressed and focus on creating better security in the AIR.

There are myriad potential threats faced by the AIR. The attacks often targeted at programs and services or hardware that can harm the data. Cyberattacks created many losses of money, data, and other resources. Most of the attacks was involving unauthorized use of computers or networks. There was an indication of evolution in a cyberattack that organizations faced in advancing malware and phishing (Donaldson et al., 2020). There are three most frequent types of security issues concerning the repositories are given are the violation of secrecy or confidentiality, integrity, and availability. Security management involves several aspects to identify threats and vulnerabilities to guarantee Confidentiality, Integrity, and access availability. Risk management also deals with threat identification and providing protection in operation, system design, and physical infrastructure (Oğüt et al., 2011). The Academic IR as a cyberspace entity is one of the objects of attack. There are hundreds of data that need to be protected; the AIR needs to consider severe attention to security issues due to this matter.

TLS/SSL Test and Security Threat and Intervention

TLS/SSL (, TLS – Transport Layer Security, SSL - Secure Sockets Layer) is a security layer that performs interception and decryption of data in the network to protect against attacks of malicious content. Data transportation is a critical issue in cybersecurity TLS/SSL is one of the tools that provides a private communication channel between networks. TLS/SSL provides the standard protocol to secure connections and safety to any classified data. However, sometimes hackers use TLS /SSL to hijack information using modified TLS/SSL protocol during information transferred (Humayun et al., 2020b; Radivilova et al., 2018). To detect TLS/SSL leaks, there should be testing to create a clean channel to decrease security risk inside that might risk being exploited by a hacker.

A secure website usually has an TLS/SSL certificate; TLS/SSL certificate is tiny data files contains cryptographic data that encrypted link between a server and a browser. The link secure all of the data passed between server and browser remain private. The benefits of using an TLS/SSL certificate on a website apart from increasing security. TLS/SSL also help to increase the website's ranking on internet search engines in search engine search results. As the front gate of the internet, the search engine announces that search results prioritize HTTPS use. The HTTPS protocol will be rated to maintain the security aspect is a top priority for search engines in ranking websites on their website Search Engine. One of the standard issues regarding the TLS/SSL is instalment. Sometimes a glitch on TLS/SSL Happens because of mixed content where TLS/SSL was installed, but not all content on the website is safe; the browser will issue a "mixed-content" warning (Taylor, 2019). Mix between secured content (HTTPS) and unsecured content (HTTP) could exploited by hackers, even though the website itself is already secured to HTTPS.

C. RESEARCH METHODS

The research methodology will use experimentation the academic AIR websites in Indonesia. This research aimed to the whole methods of security involving TLS/SSL aspect. The object of research came from the 10 best public Universities and 10 best private universities in Indonesia. The top ten universities were taken since they have the best academic repositories in their libraries. Since 2011 the Indonesian High Education Directorate General has issued a policy regarding the Uploading of Scholarly Works and Journal Articles (Liauw & Genoni, 2017b). This policy has become one of the requirements for university accreditation by the Indonesian High Education Directorate General. Using 10 best public and private university as the sample would reveal, identify, evaluate, and interpret all the AIR based on the empirical evidence and find out the missing areas and gaps in the current research, particularly in cybersecurity involving Indonesian AIR.

Academic repository is an integrated system of a university or any higher education institute. Some academic repository was connected with other system in the organization. For the safety of the universities, the name of the universities tested had been anonymized in order to keep their secure. Keeping the research object anonymity and confidentiality is one of the main responsibilities of researcher (Wiles et al., 2008). This research will keep the data anonym in order to keep away the research object in the risks of cyberattack due to the information regarding their cyber weakness on their AIR.

Cybersecurity is a complicated matters that full of confidenciality since it has many things to protect to prevent and conceal the vulnabilities of the system. The object of the research have to disguise the names of organizations and places is taken for granted in published (Guenther, 2009). The TLS/SSL provides a protocol for web client (browser) and a web server creating connection each other and using encrypted public key to agree on a shared secured key to communicate using symmetric encryption for the rest of that session.

The client created text message and the TLS in the client set up chipher suites and send it to the server. The server received and sent the SSL certificate and chipper suites. The client sent premaster secret message encoded with public key to the server. The server created the session using random and premaster secret.

The research will test the TLS/SSL protocol of AIR in higher education in Indonesia. This section explains the TLS/SSL test; the test was done between January 15th -17th, 2021. The test uses the URLs to the TLS/SSL tester tools at https://www.immuniweb.com/ssl. The main reason using the https://www.immuniweb.com/ssl tester tools to perform the test is because the website provides deep analysis of any TLS/SSL configuration and giving a good review of Indonesian AIR. The tests will give scoring from scale A to F. Scaling was also widely used in the academic environment. Once the score was got, the score will be converted to 2 to 10 (Formanek & Zaborsky, 2017b).

The scoring method was expected to give general description to the security measure in the Indonesian AIR. The data analysis based on the test score they got, the larger the score, the better the security they have. The test also gave information about the potential threat and vulnerability and recommend security intervention could be done for a better security. The type of research, model, research group, data collection techniques, validity and reliability, analysis of the data, limitations, and, if necessary, ethics committee approval should be detailed in the method section. This section aims to increase the readability and comprehensibility of the study; Under the main title of method (the general title where the research pattern is written with reference), the population and sample and/or study group should be presented under the subheadings of data collection and data analysis.

D. RESULT AND DISCUSSION

The identified AIR URL is validated by the RAMA Repository launched by the Ministry of Research, Technology and Higher Education in 2019 as the national directory of repository research results reports in Indonesia. The test gave several findings of the security condition of AIR in Indonesia. One out of the 20 repositories did not work on test due to the institution blocked any suspicious signal that made the immuniweb fail to test the TLS/SSL security. Thus, it was impossible to check on the academic repository for secured protocol or not. Graph 2 below shows that only 2 repositories use the secure protocol of the HTTPS protocol in private universities. Meanwhile, there are only 4 public universities in the public university using the HTTPS protocol in the whole AIR website. This could be a massive problem in the future since there is no protected data transfer to secure the confidentiality, integrity, and authentication of the message.

Another test manage using immuniweb was the TLS/SSL able to see the data transfer on the AIR website security through the power of the encrypted message. The test result of the private university repository is as come result as in the table below.

The test result showed most private universities AIR got an F score from the table (mean = 3.1 points which only have C in security, which means a deficient score in security issue. There are only 2 private universities in Indonesia have got a good score in immuniweb testing. The two universities got the good scoring security test because they have good administration of the AIR by the computer technical management. The computer and technical management set policies across traditional cybersecurity risk management process steps-detect, identify and respond to possible threat periodically. Meanwhile, the public university academic IR are come results follow.

The table above shows that only the public University E closed all of the system against immuniweb test for safety reasons; this policy was taken as a security policy to avoid surveillance and sniffing from any source. Based on the immuniweb test, the AIR score test also has an average score of only 3.4 or 3.7 if the Public University E out from counting, which means the AIR security issue still has C, which is C is a low standard on TLS/SSL security.

However, public universities are slightly aware of security issues with better grades in immuniweb testing than private universities. The highest score of IR security is Public University A and Public University C and Public University J because of the security management of AIR management is directly under the Data and Communication Directorate. The Directorate is directly managed the security policy for AIR include providing digital rights management, privacy, and confidentiality of the document and users, defining user behavior, and document delivery.

The immuniweb test revealed that the AIR in Indonesia is considered as "Low" protection. Most of the AIR failed to pass the test with a low score and secure messages between user and server, which can be derived from a data breach. The AIR administrator needs to be aware of this issue to ensure the data are well secured for confidentiality, integrity, and accessibility to keep privacy concerns. Several solutions need to provide stringent protections to secure and distribute sensitive data and keep the message encrypts users' information. The AIR in Indonesia also needs to state the software monitoring programs to watch traffic and identify unauthorized attempts to upload or change information or otherwise cause damage.

Overall, based on the test with immuniweb the quality of AIR security in Indonesia is deficient; this result should be considered to take mitigation action against all possibilities of threat to the AIR. Disruptions and threats can come in many ways. As one of the cyberspace entities, academic IR should learn about preventing and potential disruption and dangers lurking beyond their space. This part will discuss the potential threat and what security intervention should for the Indonesian Academic IR.

Threat over The Indonesian Academic IR

AIR played the role of accessibility to various knowledge without discrimination among the academic community using digital objects as part of most collections. Regardless of those comfort access, there is a possible threat from AIR vulnerabilities. Data risk mitigation is one of the things that the AIR administration acquired. There are many forms of data mitigation is one of them is using traffic monitor control to see patterns and the types of threats organizations are facing globally(Reeves et al., 2021). Based on AIR's investigation of AIR some potential threats could penetrate the TLS/SSL protocol. What can possibly be the threat for the Indonesian AIR involving the TLS/SSL protocol in the future?

1. Malware

Malware or Malicious ware is any type of application that made intentionally executes malicious loads on someone devices. Several softwares categorized as malware are virus, worm, Trojan horse, rootkit, and ransomware. All of them were designed to affect someone devices in different ways, like stealing data, blocked data, and breaching access (Aslan & Samet, 2020). TLS/SSL malware works with stealing the TLS/SLL keys and certificates for communication and securing communications from fraud and data exfiltration. One of the most famous scandals of data theft using malware in TLS/SSL is the Advanced Persistent Threat (APT) Heartbleed Malware. The Heartbleed malware work with reading memory systems and compromises the secret keys used to secure the service providers and reveal names and passwords of the users and other confidential data. The Heartbleed malware succeed stole digital keys and security certificates and made 4.5 million Community Health System (CHS) patient records breached to public.

In the early day, the malware was written with simple code and simple purpose and easy to detect; nowadays, malware written in a complicated code and could run deep inside the system and more complex to see but had a significant impact on the system(Aslan & Samet, 2020). However, malware threats can be anticipated by creating good traffic monitoring for malware detection with static and dynamic malware analytics to analyze the malware file using various parameters. The AIR administrator should start to consider malware as the most severe threat. Based on the findings, there are not many AIR in Indonesia did not use

any HTTPS protocol to protect their repository. Since the AIR is publicly open, there are many data is transmitted this situation is really vulnerable and could become potential malware threat to create path for information theft. Users could accidentally slip malware to the user computer or host it on its own servers, harvesting all of the user information or installing a virus.

2. The MITMA (Man in The Middle Attacks)

The TLS/SSL protocol works with securing a Web client (browser) and server during communicate each other. A web server creates secure connection between one another using encrypted public key and agree to a shared secret key to client devices, the key also used to the encrypted channel for the rest of the session. The MITMA work when a hacker has become in the middle of client and server and can imitate, intercept and access information that sends to each other (Alwazzeh et al., 2020).

The MITMA could penetrate the Indonesian AIR since most of the TLS/SSL has a problem with the keys and certificate. The AIR administrator should update the keys and certificate to keep the communication between the browser (user) and server securely. The MITMA could anticipate using a Direct Validation of Certificates (DVCert) to deploy a protocol that provides more secure certificate validation to ascertain and protect from MITMA without using third parties. Up until now The MITMA is an effective attack since it is very subtle and hard to detect. It is strongly recommended that all Indonesian AIR updated their authentication techniques, encryption and decryption algorithm.

3. Renegotiation Attack

TLS/SSL working involves two parties that communicate intensively; those two parties hold two new session keys, and sometimes change their cryptographic parameters and sometimes change authentication credentials. The two parties always negotiate regarding the changes to be made to get secure communication. This activity could be used as a stepping stone to creating an attack. The renegotiation attack allows an intruder to insert plaintext into the victim's requests by changing several procedures in the TLS/SSL. The attack uses vulnerabilities on the communication channel on TLS/SSL to tamper messages and exploits the TLS/SSL protocol, ultimately ending the security of data transmitted to the transport layer (Bijani & Robertson, 2014).

Attacks on TLS/SSL protocol can ultimately harm the data exchange since there is no authentication of the messages during the handshake phase, no verification in the arrival order of the handshake messages. The Indonesian academic IR is weak against the possibility of a renegotiation attack. A renegotiation attack could be dangerous, leading to data breaching, and could danger IR's content. The Indonesian academic IR should focus on the renegotiation vulnerability in the SSLv3. This can be done with altogether disable renegotiation on the server-side. However, securing all vulnerabilities permanently, the IR administrator should add an extension indicator for TLS to verify previous handshakes activity in all renegotiation handshakes.

Security Intervention for The Indonesian Academic IR

Security is one of the solutions to set new flows of cyber activity; security intervention could be in a broad context, a set of technical tools to improve their cybersecurity and a set of policies to repel attacks. Indonesian AIR need focus to basic security aspect but highly efficient to protect against potential threat that could mutilate AIR data. Focusing in security intervention could improve AIR services and then accelerating the task of managing cyber-attacks. There are several basic security interventions that could be implemented as strategies for Indonesia's academic IR.

1. User education

AIR users are the complicated issue in cyber security since involving human behavior. The AIR users are the essential issue where their behavior creates interaction between humans and computers. Human-computer interaction is

a set of moment decisions and create a structure of interaction to take a pile of algorithms that could lead to cybersecurity fatigue. Cybersecurity fatigue is a condition where user becomes tired or fatigue with securing their system and become neglect to the security procedure and policy (Reeves et al., 2021). Cybersecurity fatigue should not be happened on the AIR and Cyber security intervention involving user education should focused on the cyber security policy.

Indonesian AIR also needs to create a suitable security designation for the AIR from the start. Cybersecurity policy should include user behaviors that no one is expected to comply with. User security and privacy need to be designed into a system from the very beginning and coordinating from the legal aspect of local government (Donaldson et al., 2020). However, there is a lack of organizational policies and quality control in AIRs and since there were lack of privacy and confidentiality in their content (Liauw & Genoni, 2017b; Priyanto & Miksa, 2015). In this area is the users' responsibility to be more cautious and the AIR administration to provide policy and control about user works since the documents of AIR was not examined by the IR administrations.

2. Patching Policy

Patching policy involving vulnerability assessment to monitor the system and detect suspicious activity to detect unwanted access and extract the information. In the technical aspect, patching is a process to recognize and fix vulnerabilities in the system used by the organizations to prevent cyberattacks (Altaf et al., 2016). Patches are commonly used as the early process in mitigating software deficiency and vulnerabilities; implementing patches management can lower system exposures and reduce the circumstances to have cyberattack. Based on the test on finding, several issues addressed with patching management. The findings indicated that most of the AIR do not modernized the TLS/SSL certificate regularly, including their software use to secure the connection. Patches is an essential process not only to fix software deficiency, but also give a new capability to to secure the data (Altaf et al., 2016). Patching management implementation periodically is crucial since the cyberattack method has become complicated and advanced in many ways and in many forms. Patching management could be hard since it involved significant resources, However, current development of technology there are myriads of option ways to keep the system up-to-date even automated patch management tools can help cyber security analyst detect vulnerability and maintain the system up-to-date against the latest threats.

3. Create strong encryption

Encryption is an old practice of creating a message that is only read to the intended recipient, usually using scrambling a message (Alashwali & Szlachowski, 2018). Encryption is the essential process of TLS/SSL; this process involves the server to interact with users through a secure environment. Based on findings the AIR had many problems with encryption, particularly with the security certificate as a key which is the final stage in the SSL Handshake process. The Indonesian AIRs need to enforce policies regarding each session key that is used for secure communication. Indonesian AIRs urge to update the certificates on their TLS/SSL system. The policy to create a firm encryption policy should be carried out through strengthening technical standards and operating procedures for the academic IR. Therefore, it feels to implement encryption technologies. It is fundamentals for creating a standard encryption policy to properly align the organization with its business process resources so that encryption technology is applied consistently across the organization (Abrenio, 2018). In the future Indonesian Academic IR needs to have proper planning, implementation, and monitoring of the standard encryption policy to ensure the sustainability of strong encryption as a security control to protect their information asset.

E. CONCLUSION

The AIR is an entity of cyber environment that needs to be acknowledged its security since it preserves its users' knowledge and personal

record. Thus, cybersecurity is a basic necessity of an AIR. However, up until now, research involving AIR security are still scarce. As one of the most prominent AIR in the world on the open access movement, Indonesia is still left behind on the cybersecurity of AIR. Current technology has brought up some complicated problems in security issues. Based on the security assessment, Indonesian AIR is still vulnerable in several aspects of security, particularly in TLS/SSL. Most Indonesian AIR have not updated their AIR system into the latest update TLS/SSL standards; this made the Indonesian AIR have a low assessment score on the TLS/SSL assessment. Cyber security issue has become a prominent issue that should be drive up to the AIR stakeholders to create better understanding about cyber security issues since it directly involves to the national security. User education to prevent cyber fatigue, patching management periodically and strong encryption policy are several recommendations of this early research to create greater cyber security for AIR in Indonesia. Further research also to be conducted regarding the security issue of the Indonesian academic repository and other cyber entities involving education in Indonesia. This research is just preliminary which has limitation in every aspect. There are widely opportunities in the future to conduct research involving Cybersecurity and AIR to create a better implementation of AIR that protect the information asset of Indonesian higher education institution.

REFERENCES

Abrenio, G. (2018). *How to develop an enterprise encryption policy*. Cyberarmed. https://www.cyberarmed.com/how-to-develop-an-enterprise-encryption-policy/

Agrawal, B., & Jain, A. (2018). Missing Values Prediction for Cyber Vulnerability Analysis in Academic Institutions. *International Journal of Computer Applications*, *180*, 16–25.

Alashwali, E. S., & Szlachowski, P. (2018). Risks and Security of Internet and Systems. In F. Cuppens (Ed.), *13th International Conference CRiSIS 2018*. Springer.

Altaf, I., Ul Rashid, F., Dar, J. A., & Rafiq, M. (2016). Vulnerability assessment and patching management. *International Conference on Soft Computing Techniques and Implementations, ICSCTI 2015*, 16–21. https://doi.org/10.1109/ICSCTI.2015.7489631

Alwazzeh, M., Karaman, S., & Shamma, M. N. (2020). Man in The Middle Attacks Against SSL/TLS: Mitigation and Defeat. *Journal of Cyber Security and Mobility*, *9*, 449–468. https://doi.org/10.13052/jcsm2245-1439.933

Aslan, O., & Samet, R. (2020). A Comprehensive Review on Malware Detection Approaches. *IEEE Access*, *8*, 6249–6271. https://doi.org/10.1109/ACCESS.2019.2963724

Bijani, S., & Robertson, D. (2014). A review of attacks and security approaches in open multi-agent systems. *Artificial Intelligence Review*, *42*(4), 607–636. https://doi.org/10.1007/s10462-012-9343-1

Donaldson, S., Navin Shah, J., Pedley, D., Crozier, D., & Furnell, S. (2020). *UK Cyber Security Sectoral Analysis 2020*.

Formanek, M., & Zaborsky, M. (2017a). Web interface security vulnerabilities of selected European open-access academic repositories. *LIBER Quarterly*, *27*(1), 45–57. https://doi.org/10.18352/lq.10178

Formanek, M., & Zaborsky, M. (2017b). Web interface security vulnerabilities of selected European open-access academic repositories. *LIBER Quarterly*, *27*(1), 45–57. https://doi.org/10.18352/lq.10178

Guenther, K. M. (2009). The politics of names: Rethinking the methodological and ethical significance of naming people, organizations, and places. *Qualitative Research*, *9*(4), 411–421. https://doi.org/10.1177/1468794109337872

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020a). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, *45*(4), 3171–3189. https://doi.org/10.1007/s13369-019-04319-2

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020b). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, *45*(4), 3171–3189. https://doi.org/10.1007/s13369-019-04319-2

Kavallieratos, G., & Katsikas, S. (2020). Managing cyber security risks of the cyber-enabled ship. *Journal of Marine Science and Engineering*, *8*(10), 1–19. https://doi.org/10.3390/jmse8100768

Kemristekdikti. (2020). *RAMA Repository*. https://rama.ristekbrin.go.id/

Kovářová, P. (2011). Vulnerabilities of institutional repositories. *Seminar on Providing Access to Grey Literature 2011*, *July*.

Liauw, T. T., & Genoni, P. (2017a). A Different Shade of Green: A Survey of Indonesian Higher Education Institutional Repositories. *Journal of Librarianship and Scholarly Communication*, *4*(0), 0–26. https://doi.org/10.7710/2162-3309.2136

Liauw, T. T., & Genoni, P. (2017b). A Different Shade of Green: A Survey of Indonesian Higher Education Institutional Repositories. *Journal of Librarianship and Scholarly Communication*, *4*(0), 0–26. https://doi.org/10.7710/2162-3309.2136

Mita Paul & Anindya Basu. (2015). a Study on Open Access in Indonesia. *International Journal of Library Science and Research (IJLSR)*, *5*(4), 11–20.

Noorden, R. Van. (2019). *Indonesia tops open-access publishing charts*. https://www.nature.com/articles/d41586-019-01536-5

Oğüt, H., Raghunathan, S., & Menon, N. (2011). Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. *Risk Analysis : An Official Publication of the Society for Risk Analysis*, *31*(3), 497–512. https://doi.org/10.1111/j.1539-6924.2010.01478.x

Perpusnas. (2020). *Indonesia One Search*. http://onesearch.id

Priyanto, I. F., & Miksa, S. D. (2015). Readiness of Indonesian academic libraries for open access and open access repositories implementation: A study on Indonesian open access repositories registered in OpenDOAR. *ProQuest Dissertations and Theses*, 207.

Radivilova, T., Kirichenko, L., Ageyev, D., Tawalbeh, M., & Bulakh, V. (2018). Decrypting SSL / TLS Traffic for Hidden Threats Detection. *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 2–5.

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue. *SAGE Open*, *11*(1). https://doi.org/10.1177/21582440211000049

Taylor, A. (2019). Decrypting SSL traffic: best practices for security, compliance and productivity. *Network Security*, *2019*, 17–19. https://doi.org/10.1016/S1353-4858(19)30098-4

Wiles, R., Crow, G., Heath, S., & Charles, V. (2008). The Management of Confidentiality and Anonymity in Social Research. *International Journal of Social Research Methodology*, *11*(5), 417–428. https://doi.org/10.1080/13645570701622231

Zervas, M., Kounoudes, A., Artemi, P., & Giannoulakis, S. (2019). Next generation Institutional Repositories: The case of the CUT Institutional Repository KTISIS. *Procedia Computer Science*, *146*, 84–93. https://doi.org/10.1016/j.procs.2019.01.083

FIGURE LIST

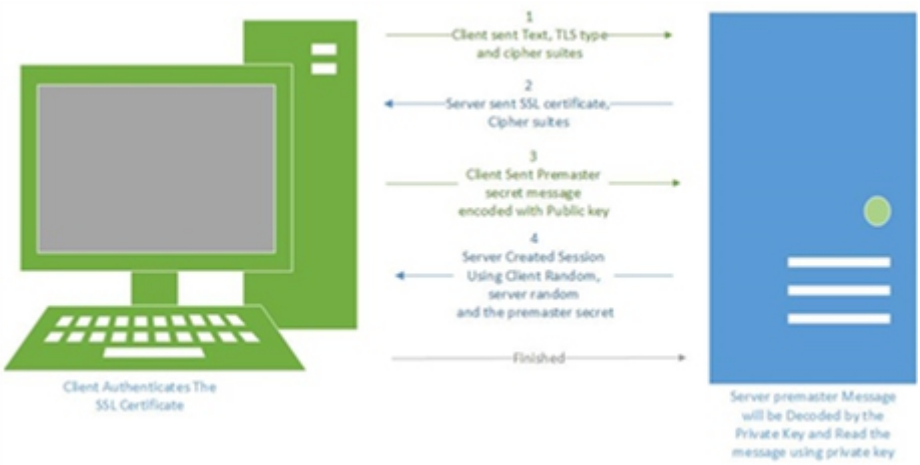

Figure 1. TLS/SSL Working Scheme
(Source : Alwazzeh et al., 2020).

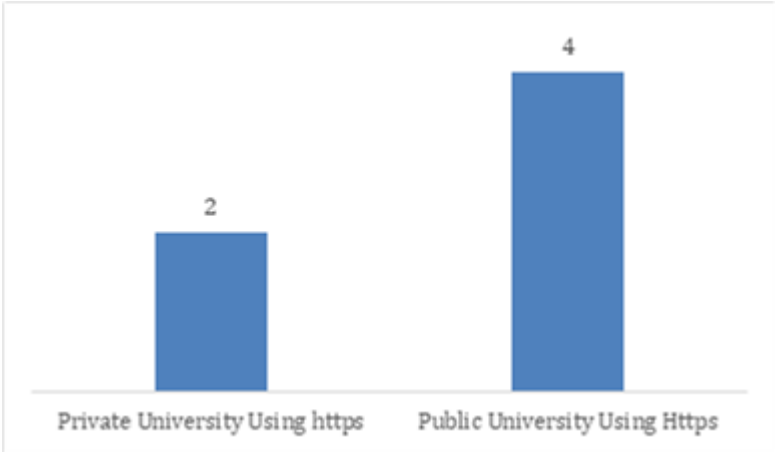

Figure 2. Graph composition on HTTPS protocol among private and public university
(Source: Testing Result on Immuniweb)

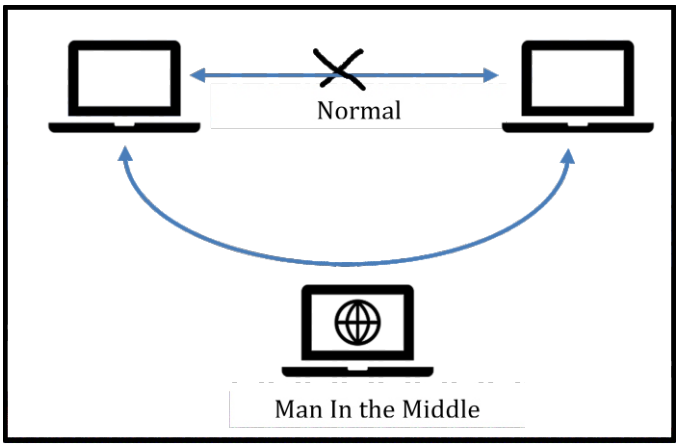

Figure 3. Man In Middle Attack Scheme
(Source : Alwazzeh et al., 2020)

TABLE LIST

Table 1. Testing TLS/SSL Score

TLS/SSL test	Converted score
A+	10
A	9
A-	8
B+	7
B	6
B-	5
C+	4
C	3
F	2

(Source: Formanek., 2017)

Table 2. TLS/SSL Scoring test at private universities

No.	University Name	SSL Test Score Immuniweb	Points Score
1	Private University A	A+	10
2	Private University B	C	4
3	Private University C	F	2
4	Private University D	F	2
5	Private University E	F	2
6	Private University F	F	2
7	Private University G	B-	5
8	Private University H	F	2
9	Private University I	F	2
10	Private University J	F	2

(Source: AIR Testing Result from Immuniweb)

Table 3. TLS/SSL Scoring test at public universities

No.	University Name	SSL Test Score Immuniweb	Points Score
1	Public University A	B-	5
2	Public University B	F	2
3	Public University C	A-	8
4	Public University D	F	2
5	Public University E	N	-
6	Public University F	F	2
7	Public University G	F	5
8	Public University H	F	2
9	Public University I	F	2
10	Public University J	B	6

(Source: AIR Testing Result from Immuniweb)