2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON) | 978-1-6654-9602-5/22/$31.00 ©2022 IEEE | DOI: 10.1109/COM-IT-CON54601.2022.9850702

DATA SECURITY AND PROTECTION: A MECHANISM FOR MANAGING DATA THEFT AND CYBERCRIME IN ONLINE PLATFORMS OF EDUCATIONAL INSTITUTIONS

Abubakar Mohammed [1],Sanjeev Kumar[2],Hammandikko Gaya Mu'azu[3], Rajiv Kumar [4], Praveen Shah[5], Minakshi Memoria[6],Amarjeet Rawat[7],Ashulekha Gupta[8]

[1]Department of Information Technology, Federal University Dutse-Nigeria
[1]ajungudo@mautech.edu.ng
[2]Department of Computer Science & Information Technology, Himgiri Zee University, Dehradun,India
[2]sanjeev_solanki@live.in
[3]Department of Statistics and Operations Research, Modibbo Adama University Yola, Nigeria
[3]hdikko2017@mautech.edu.ng
[4,5,7]Department of Computer Applications,Uttaranchal Institute of Management,Uttaranchal University,Dehradun, India
[4]rajiv.gill1@gmail.com, [5]praveenshah@uttaranchaluniversity.ac.in,[7]aj.amar.rawat@gmail.com
[6] Department of Computer Science and Engineering, Uttaranchal Institute of Technology , Uttaranchal University, Dehradun, India
[6]minakshimemoria@gmail.com
[8]Department of Management Studies,Graphic Era Deemed to be University , Dehradun, India
[8]ashulekha26@gmail.com

Abstract— ***Advancement in technology has brought changes in educational institutions that leads to the adoption of several information system and online platforms. Students and staff were sharing important data through these platforms. This has exposed the institution to cybercrime activities by both internal and external agents of malicious users. Their motive is to gain access to the platforms in order to data related to fees and other academic records, or to distort the entire system to steal the data with the aim of committing an illicit transactions or activities. This paper aimed at providing security mechanism or model for data security and protection in educational institutions. It provides empirical studies related to data security and protection as well as cyberspace and online data theft in educational institutions. The paper recommends that educational institutions should adopt and implement the security mechanism and models to prevent cybercrime activities. It also recommends that sensitization should be organized for both students and staff on the use online platforms to prevent them from being exposed to malicious users.***

Keywords— ***Cybercrime, Cyberspace, Data Security and Protection, Educational Institution, Online Platforms.***

I. INTRODUCTION

Cybercrime and online atrocities have become rampant nowadays. People tend to use their smart devices in committing cybercrime. Cybercrime and online data stealing occurred as a result of failure in data security and data protection. Criminals take advantage of these failures and mount their attack on users.

Data security can be seen as a field of science that deals the study of data protection methods in both computer and communication systems. It involves several kinds of controls about data such as cryptographic, access, information flow, and inference controls. It also contains backup and recovery plans [1]. Data security is all about ensuring safety of data from any malicious or accidental damage. It means protecting data from being lost or theft [2].

Educational institutions use various online platforms that stores both students and staff data. If proper security and protection mechanism is not provided, the data may be stolen or damaged by the cybercrime perpetrators. The institutions need to provide strong and reliable mechanism that will protect the integrity of the stored data. The integrity of data is the most critical element in any information system. Since educational institutions uses information system which sometimes, they even use cloud-based information systems, protecting their data from unauthorized users or distortion as well as modification is one of the major steps in providing data integrity [3].

Therefore, this paper aimed at providing empirical studies on data security and protection, cyberspace and data theft. It will also provide a security model to be implemented when providing security and protection of data in educational institutions. The paper is review research that uses secondary sources of data from journal articles.

II. Overview of Data Security and Cyberspace Data Theft

Setting up appropriate and reliable data security measures will ensure maximum confidentiality and integrity of data which in turn will guarantee data protection [4].

Security of data may have different perspective such as physical security, password and encryption. Physical security entails dealing with environments or rooms where devices that stored the data are kept. Access to such places should be determined by the authorized persons. Computers and other devices should be protected with strong passwords. In addition to the password protection, certain data need to be encrypted or shield so that it cannot be decrypted easily by the intruders. This will ensure adequate security and protection of the stored data [2].

Effective data security and protection strategies will strengthen the trust of people in their respective organizations. It will give quick response when there is breach of security or trusts. The strategies are applicable based on the kind of data the organizations collected and stored [5]. For educational institutions, data related to students and staff are usually collected and stored. This may include students' enrollment data, fees and academic record data, staff human resource and payroll data, etc. Some of the security strategies may include taking inventory of the data classification, where the data will be stored along with specification and format, and how the data can be accessed by the authorized persons [5].

Data security measures provide mechanism for managing accidental destruction of data as well as deletion or modification through the access control process or procedures. It gives privileges that can be enforced to users. These privileges may be added, changed or revoked from the already assigned users. The concept determines what users can do within information systems [6].

Nowadays, large volume of data is being stored on the cloud. It leads to the innovation of cloud computing. Security and protection of such data is paramount in order to avoid malicious users from distorting the data. Some security issues related to data on cloud include compliance, privacy, trust, and legal matters. Security of the data is more complex and complicated in cloud computing than in traditional information system. This is because, the data are been scattered and disintegrated on different machines and storage devices which may include servers, personal computers, and other smart devices such as sensor networks and phones [3].

The emergence of internet and computing technological advancement has increase the rate of cybercrime and other online data theft. Criminals usually perfects their crime acts through the internet facilities. Crime activities such as identity and data theft, fraud, hacking, money laundering, child pornography, etc. are achieved through the use of internet. Websites and other online facilities like emails and chat rooms (social media platforms) give criminals chance to steal data or information of users and commit illicit transactions or activities to the detriment of these innocent users [7].

Educational institutions tend to adopt innovative technologies in rendering teaching and learning activities as well as other administrative issues. This leads to implementation of many online platforms that handle such services. However, the institutions have engaged in the battle of protecting the online data due to the activities of cyber criminals. Most of the cyber attacks on the educational institutions are done by both internal and external agents with the aim of data modification, alteration or distortion. The internal agents may be students or staff of the institutions that may infiltrate the system in order to alter data related to fees, academic records, etc. The external agents may be competitors or malicious attackers that will infiltrate the system to create havoc [8].

In their effort to explore more information system and technology to handle educational activities, several online or e-learning platforms were adopted by these institutions for flexibility and easy access by both students and teachers during learning process. However, implementing these technologies requires a lot of strategies by educational institutions towards data protection and security. This require building a trusted and secure environment for sharing data and other learning resources [9].

III. Security Mechanism for Managing Data Security and Data Theft

The section provides the security mechanism that can be used in developing data security model for managing and protecting data in educational institutions. The mechanism is presented in the table below [6]:

Table 1: Security Mechanism

Component	Elements of the Component	Action	Remark
Authentication	Access Parameters: - Username - Password - Biometrics	Require authorization and verification before accessing data storage platforms	Both students and staff are involved
Access Control	Permission	Applicable to both online and offline platforms	Both students and staff are involved
Encryption	Security models	Shielding/covering data to be decrypted by the intended recipients	Require technical expertise
Backup	Online and offline backup strategies	Regular storage of data to another specified location and device	Both students and staff are involved

Table 1 above provide security mechanism to be observed and implemented in educational institutions for safeguarding data of information systems and other online platforms within the institutions. The table contains four components namely authentication, access control, encryption, and backup. The authentication consists of access parameters that gives users

chances of operating systems implemented within the institutions. These parameters include username, password, and biometrics. Every user requires a username and password to gain access to the system. User will register and create unique login details (username and password). The password parameter may have further verification by means of One-Time-Password (OTP) where verification code will be sent to the registered mobile number or email ID of the user whenever there is attempt to login by the existing parameters (username and password). Once the user entered the OTP, the system will authorize him/her automatically. The OTP is a temporary code that last for a shorter period, it expired once the validity period elapsed. In addition to the username and password, biometric features will be added to capture the users' finger prints and facial recognition to further strengthen the security of the system and protect the stored data from being stolen or distorted.

Access control is another component that grants users permissions to commit or perform activities within the system. Some users may just be able to view or read data, while others may be able to add, change, or conduct all operations. Administrators can determine the level of user involvement on the platform. This permission involved both offline and online platforms. The offline platform may be laboratory teaching tools or computer systems within the local area network, and the online platforms may the E-learning applications that contains the Learning Management System (LMS) as well as the information system that host the students record management system and results portal.

Other components include encryption which require additional security features to be added to the data or message when sending among users. It involves encoding or shielding the message so that nonrecipient cannot understand content of the message. It can only be decrypted or decoded by the intended recipients of the message. This component requires the expertise knowledge by both the sender and the receiver of the message on the encoding technique used. The last component on the table is backup. It requires periodic storage of the stored or collected data to another device in another safe location. The backup strategy may be both online and offline. The online backup requires cloud services so that it can be accessed anywhere and anytime without physical movement with the storage device. The offline backup requires saving the data on another removal device to be kept in another location, or saving the soft copy of the data or applications on another system separately with the same functions.

Protection of information contents and resources using different categories of stored data for possible processing and transmission via computer systems or networks is referred to as information security [10]. In ensuring security and protection of data, varieties of tools and strategies are need such as [11]:

a) Firewalls: Firewalls filter and report traffic data to the monitoring and detection systems put in place for controlling and ensuring security of information.
b) Security Incident and Event Management (SIEM): SIEM solutions are used in providing aggregate data particularly on the logging events for threat detections. It is mostly used for testing security compliance and performance optimization.
c) Data Loss Prevention (DLP): DLP strategies protect data from loss or being modified. This involves data categorization, backup and data sharing.
d) Intrusion Detection and Prevention System (IDPS): IDS technology monitors and detects incoming traffic and threats. Any suspicious activities will be evaluated and alert will be sent to the central monitoring systems.
e) User Behavioral Analytics (UBA): This technology collect data on activities of users and matches it with their behaviors. Baseline activities will be made to detect inconsistencies for potential threats.
f) Endpoint detection and response (EDR): EDR technology help users to monitor endpoint activities to identify suspicious threats and provide automatic response. The technology is meant to improve visibility of the endpoint devices. It works with data collected from logging events.

IV. Conclusion

Security and protection of data is important in every organization. Advancement in technological innovations lead to the adoption of several online platforms in educational institutions which has exposed them to cybercrime and online data theft by criminals. This paper has provided empirical studies on the data security and protection as well as cyberspace and online data theft activities in the educational institutions.

Despite the security mechanism provided in this paper, educational institutions need to sensitize both students and staff on the use of available online resources and platforms within their respective institutions to prevent them from being exposed to the malicious users. The security strategies and models should be adopted and implemented by the educational institutions in order to solve or minimize the activities of cybercrime perpetrators.

References

[1] D.E. Denning. Cryptography and Data Security. Addison-Wesley Publishing Company, California, 1982. Retrieved from: https://faculty.nps.edu/dedennin/publications/Denning-CryptographyDataSecurity.pdf on 20th January 2020.

[2] CESSDA. Data Security. Consortium of European Social Science Data Archives. Parkveien 205007 Bergen, NORWAY. Retrieved from: https://www.cessda.eu/content/download/243/2401/file/CESSDA%20User%20Guide%20for%20data%20management_6_Data%20security.pdf on 20th January 2020.

[3] Y. Sun, J. Zhang, Y. Xiong, and G. Zhu. Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks, Vol. 2014. Retrieved from: https://www.researchgate.net/publication/274230804_Data_Security_and_Privacy_in_Cloud_Computing on 10 February 2020.

[4] UNHCR. Policy on the Protection of Personal Data of Persons of Concern to UNHCR. Data Protection Policy, The UN Refugee Agency. Retrieved from: https://www.refworld.org/pdfid/55643c1d4.pdf on 20th January 2020.

[5] D.R. Drye, LLP. Warren, and D.Z. Cave. Data Security Made Simpler. NACHA – The Electronic Payments Association, 2010. Retrieved from: https://www.visa.com/visariskproducts/downloads/bbb-visa-data-security.pdf on 15th February 2020.

[6] D.E. Denning and P.J. Denning. Data Security. Computer Surveys, Vol.11 No.3, September 1979. Retrieved from: http://www.sis.pitt.edu/jjoshi/IS2935/Fall04/p227-denning.pdf on 25th December 2019.

[7] N. AbdulManap, A. AbdulRahim, and H. Taji. Cyberspace Identity Theft: An Overview. Mediterranean Journal of Social Sciences, Vol.6 No.4 S3, August 2015. Retrieved from: https://www.researchgate.net/publication/282465632_Cyberspace_Identity_Theft_An_Overview/link/568e034008aeaa1481ae80e6/download on 20th January 2020.

[8] M.J. Maranga and M. Nelson. Emerging Issues in Cyber Security for Institutions of Higher Education. International Journal of Computer Science and Network, Vol.8 Issue 4, August 2019. Retrieved from: https://www.researchgate.net/publication/335664780_Emerging_Issues_in_Cyber_Security_for_Institutions_of_Higher_Education/link/5d729c32299bf1cb808b4629/download on 15th February 2020.

[9] I. Badara, F. Ioras, and K. Maher. Cyber Security Concerns in E-learning Education. Proceedings of ICERI 2014 Conference, 17th – 19th November 2014, Seville, Spain. Retrieved from: http://ecesm.net/sites/default/files/ICERI_2014.pdf on 20th March 2020.

[10] R. Kumar and M. Memoria, "A review of memetic algorithm and its application in traveling salesman problem," Int. J. Emerg. Technol., vol. 11, no. 2, pp. 1110–1115, 2020

[11] R. Kumar, "A survey on memetic algorithm and machine learning approach to traveling salesman problem," Int. J. Emerg. Technol., vol. 11, no. 1, pp. 500–503, 2020,

[12] R. Kumar, "An experimental analysis of explorative and exploited operators of genetic algorithm for operating system process scheduling problem," Int. J. Eng. Technol., vol. 2, no. 6, pp. 472–476, 2010.

[13] R. Kumar, M. Memoria, and A. Chandel, "Performance Analysis of proposed Mutation Operator of Genetic Algorithm under Scheduling Problem," 2020, doi: 10.1109/ICIEM48762.2020.9160215.

[14] R. Kumar and M. Memoria, "Analysis of available selection techniques and recommendation for memetic algorithm and its application to TSP," Int. J. Emerg. Technol., vol. 11, no. 2, pp. 1116–1121, 2020,

[15] R. Kumar, S. Gill, and A. Kaushik, "An impact of cross over operator on the performance of genetic algorithm under operating system process scheduling problem," 2011, doi: 10.1109/CSNT.2011.150.

[16] R. Kumar, M. Memoria, A. Gupta and M. Awasthi, "Critical Analysis of Genetic Algorithm under Crossover and Mutation Rate," 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), 2021, pp. 976-980, doi: 10.1109/ICAC3N53548.2021.9725640.

[17] A. Gupta, R. Parmar, P. Suri and R. Kumar, "Determining Accuracy Rate of Artificial Intelligence Models using Python and R-Studio," 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), 2021, pp. 889-894, doi: 10.1109/ICAC3N53548.2021.9725687.

[18] R.P. Romansky and I. S. Noninska. Challenges of the digital age for privacy and personal data protection. Mathematical Biosciences and Engineering, Vol. 17 Issue 5, August, 2020.

[19] O. Cassetto. Information Security (InfoSec): The Complete Guide. Information Security, February 2022.