Review Article

Students' Academic Record Systems and Their Security Issues

ABSTRACT

Students' academic records are an invaluable resource for universities and collegesworldwide, yet, their safekeeping is still a major concern formany of these institutions. The security measures currently applied to protect students' academic record systems are deemed unsatisfactory. This paper surveys the security issues relating to students' academic record delving into existing students' academic records systems, cybersecurity challenges and broader securityconcerns. The paper further proposespractical security mechanisms to address these security issues with the aim toempoweracademic institutions to build and maintain strongly protected academic record systems for capturing, storing and retrieving studentacademic data.The work underscores the urgent need of educational institutions toexertextra efforts to securely maintain students' academic records and facilitate easy access and use by various stakeholder in the educational space.

Keywords: *Student academic record, Information system, Cyber security, Information protection*

1. INTRODUCTION

Educational and training centres all over the world maintain records about students in many forms including, "handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche" [1]. The information encompassesstudents' personal information (date of birth, parents or guardian name and addresses, emergency contact numbers, previous schools attended etc.), grades, test score, areas of specialization, disciplinary records, medical and health records, class attendances, previous academics awards, co-curriculum engagements and more.

Recordkeeping in schools traditionally is supported in two main categories – manual and computerized [2]. Manual systems for academic recordkeeping were originally popular but gave way to computer-based records systems due to their many shortcomings. For instance, in a manual system, data is entered manually exposing it to entry errors. Additionally, analysing the often-long list of information requires laborious hand counts,leading to inefficiencies and low productive.The rapid proliferation of microcomputers hasestablished them as the dominant tool for recordkeeping in schools [2].

A student record system is a computerized systemdesigned for tracking and maintaining records of student information including attendance, exam grades, and conduct. Computerized academic records systems help store students'recordson "electronic storagemedia that can be readily accessed or changed" [3].These systems are tailored to provide different access privileges to students, teachers, administrators, and in some cases parents to search and retrieve stored data on students' academics and personal information [4].The essence is to nurture a well-informed student body about their academic progression fostering their ability to follow instructions and ask pertinent questions about their academic life. Empowering students with such capabilities encouragetheir active involvement in their own development, strengthen the student-university relationship and fosters effective school management.

However, providing accurate, reliable and trustworthy academic records is a difficult task for many educational institutions in their quest to fulfil evidential requirements [5]. The National Archives of Australia [6] notes that students' academic records must be reliable and available permanently. Attwood and Gill in [7]assert lack of funds and material resources for recording keeping, inadequate qualified personnel and facilities, and growing student population room space are common causes of concern for heads of educational institutions regarding proper record keeping.

The security of students' academic records has emerged asa significant and widely acknowledged concern in educational institutionsdrawing attention from scholars and practitioners alike [8][9]. Academic institutions find themselves grappling with the magnitude of unresolved security issues surrounding the safe use of students' academic record systems and the imperative to

safeguard the information contained within [9]. The prevalent security challenges associated with students' academic records are outlined below:

1.1 *Masquerading user identity*

Masquerading occurs when any entity deceptively assumes the identity of a genuine entity. By so doing, the belligerent entity is able to gain control of privileges thatit otherwise won't have. In respect of academic records system, an actor, whether a student or tutor or some other school-related actor, may masquerade as another to gain entry into a file or storage device to which it has no legitimateauthorization. Such a masquerading user will act deceptively to reach their desired goal.

1.2 *Unauthorized use of systems resources*

Aside masquerading, a different type of assault on academic records occurs when an attacker gains unauthorizedentry into a resource either via a network or on an actual computer holding the academic resource. This form of attack specifically targets accessing files, computer storage or the processing hardware of a computer without proper authorization. In network setting, an attacker might expose and use a network resource such as a shared printer, a shared application program or all or some of the data held in a database along with its accompanying applications.

1.3 *Unauthorized disclosure and transmission of academic data*

This type of system attack occurs when there is inadvertent disclosure and subsequent transmission of internal or external information that has been processed and heldon a network to any party without the needed authorization to read thatpiece of stored information. Unauthorized disclosure could arise, for example, during information collection and storage through computers or the theft of storage devices. The risks associated with unauthorized disclosure may range from low, to medium to high and with varying degree of impact.

1.4 *Unauthorized alteration ofacademic data*

Illegitimate tampering the academic records of students or other academic or administrative documents is considered a severeviolation in many educational institutions. Unauthorized alteration can lead to dire repercussions. These unauthorized changes are often a deviation from known conditions with the intention tosurreptitiously alter the physical or logical nature of data or the physical network.Such alteration may take place within a system or take place over a network. Other manifestation of this attack includes unauthorized addition or removal of a resource into or from a records system, unauthorized destruction, modification and exposure of records pertaining to a student's academic history. If a student's academic data or its supportinghardware changes, it poses a significant risk to confidentiality, integrity and availability with potentially grave consequences.

1.5 *Repudiation of actions on academic records systems*

The repudiation of actions attack seeks to circumvent the accountability processes within an organization regarding the use of academic records. Its main purpose is to aid a malicious entity to refute responsibility for an act over a system, say an academic record system. This attack can be engineeredat both the sender and receiver ends of a records system. For example, if a student may request a transcript of results and then later deny having made such a request despite requested document was indeed delivered to him or her.On the other hand, a repudiation of action will arise if an officer in charge of processing such a request later denies receiving such a transcript production request. Such actions undermine the trust between students and academic service providers.

1.6 *Denial of service attack*

Denial of service attacks are planned to obstruct an authorized actor in an academic records management system the privilege of accessing and usingresources or services available to them.In the context of academic record, denial of service could involve the deliberate locking of academic files containing the essential details of a student, thereby denying the student use of the file. In addition, an attacker employing this approach may inundate a network with redundant messages causing the targeted user to be overwhelmed with messages with no real value.This disruption in the record-keeping processes will impede authorized personsfrom gaining access to the necessary academic data.

This paper will explore some existing students' academic record systems, their security features, and security concerns. As a way of strengthening the security architecture of students' academic records, we will proposesome better approaches to confront those security issues. The ultimate goal is to provide practical suggestions that educational institutionscan implement for more securestudents' academic records systems.

The remainder of the paper is presented as follows: In the next section, we will present and describe existing systems for keeping academic records of students. The section afterwards will dissect the access and security of academic records systems. In the final section, we will propose ways of enhancing the security ofstudents' records in educational institutions.

2. REVIEW OF ACADEMIC RECORDS SYSTEMS

2.1 Students' records system

A student record encompasses information directly related to a specific student, which is held in variousformats and media held by academic institutions on behalf of the student during their study period (FERPA, Act 1974). These records may originate from a student, a representative acting on their behalf or by the educational institution itself. Student recordsmay be classified as educational or non-educational. Educational information includesdetails about the academics, admission, financial aid, discipline, and counselling. Non-educational records encompass employment, medical, law enforcement, alumni records and the likes.

Educational establishments collect, organise and maintain students records which may exist in paper-based or automated formats. Irrespective of the medium, well established students' record system offers numerous benefits. Firstly, it empowers decision-maker with the ability to generate and retrieve information about students, an entire academic unit and even an institution as a whole. Secondly, an automated student record system facilitates processing and distribution of students'records between universities and collaborating institutions. Moreover, effective integration of students' records system with other staff data, resources and financesenhances management functions. A well-designed student records system playspivotal role in the smooth operation of an education system enabling academic institutions to fulfilstudent's academic aspirations during their time in school and after school.

The integration of separate students' records culminates in a comprehensive student record system. This system provides functionalities such as entering, deleting, or updating records, generating reports such as transcripts of results, performing analyses and supporting various decisions making processes. Students' record systemscan be maintained as a collection of paper files, in a filing cabinet or built in, microfilm or electronic files stored in computing storage media. Many educational institutions, recognising the advantages offered by computers have embraced automated databases for the efficient and secure management of student records.

2.2 Access to students' academic records

Educational institutions worldwide are either implementing or are on the verge of implementing systems tosafely manage students' academic records. This endeavour is to afford students and educational actors avenues to access information tailored to their needs.Granting studentsaccess to their academic information fosters a strong connection between them and the school administration ensuring they stay well-informed about their academic progress.However, while is it necessary to provide students access to their own data, the issue of confidentiality must be carefully considered. Information stored on and accessible over computer networks remains susceptible to access by different individuals posinga concern for IT departments. There are three kinds of records for administrative purposes[10] as mentioned below.

2.2.1 Active records

These are current records routinely used in an institution to support its administrative functions and for decision-making processes. Within this category, certain records are confidential while others are non-confidential and are available for routing references and usage. This distinction is crucial in maintaining the balance between transparency and data protection with regards to academic records.

2.2.2 Semi-Active records

These are occasionally used records yet take up useful storage or office space. These records are better placed in backup storage devices or adjoining offices away from the main storage centres in

the case of manual records. The ensure is space to allocate to the frequently accessed and essential records.

2.2.3 Inactive records

These records are rarely used for the daily operations of an institution but harbour valuable information on the institutions working and functions carrying potential research or historical significance. Their disposal demands careful considerationdue to their utility during emergencies to support the uninterrupted operation of the institution.

Different actors in the educational space may be granted different access to any of these record types on a case-by-case basis.Student for instance can request for their semester results or fee payment history and it falls upon an authorized officer to interpret and provide the requested information to the student. Student may then apply to review the record. Parents ofdependent students may also make requests for information about their wards and staff members may seek access for legitimate records needs. External bodies, such as prospective employers, may seek specific portions of a student's record. It is important that any information released about a student is for non-commercial reasons and is accompanied by proper written consent. Figure 1 visualizes the diverse actors who may access information pertaining to a student's academics.

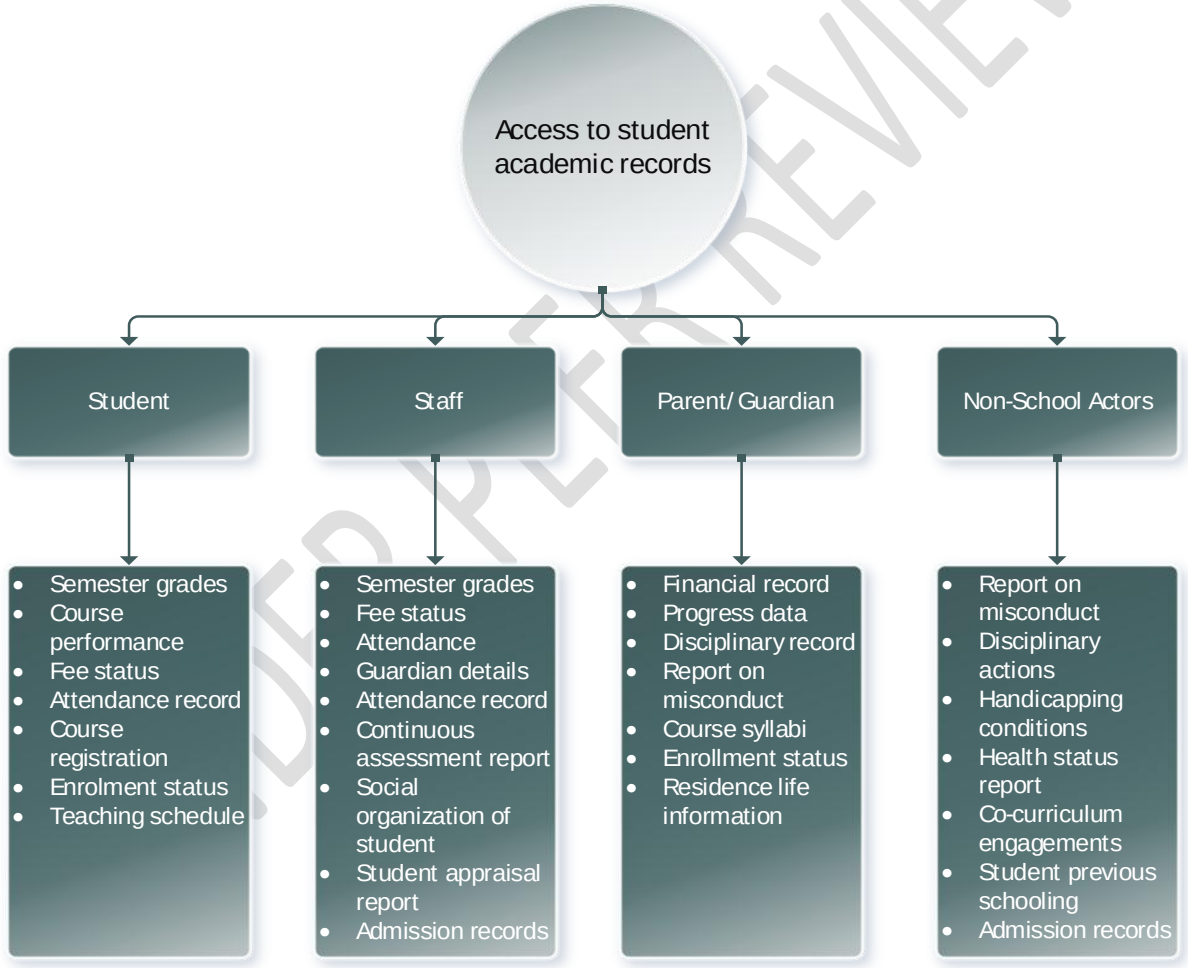

Fig. 1. Educational stakeholder with their possible reason to access students' academic records.

2.3 Risk associated with poor management of academic records

The robustness of a student records system hinges heavily on effective and efficientof the establishedrisk management processes. Early identification of risks enhances the authenticity and integrity of records [11]. It is therefore pertinent to integrate recordkeeping into an institution's overall risk management process. A deficient records management process mayexpose departments of an institution to various risk. While paper-based records management was less burdensome, the current trend in digitization and computerization, bring new layers of complexity to record management in

educational institutions. In this new way of records management, challenges presented include, “managing access, versioning, controlling and surrogates.”[12]. Consequently, it is imperative to shift from viewing the management of academic records as solely an IT department function to considering it as an institution-wide affair with a broader and consultative mandate.

From the outset, it is essentialto identify aspects of records management that poses risk to an institution or have significant cost implication on the institution.Unfortunately, proper records management often receives insufficient attention in many institutions. According to Ngoepe in [13],poor or lack of proper recordkeeping exposes an institution to four kinds of risks. These risks are legal, financial, reputation and information loss. In many educational institutions, it is common to find an individual employee solely in charge of and possessing critical information. The risk of information loss is high when such an individual leaves or resigns, astransferring such privileges and control to another employee if often challenging. The authority to handle and release information about students’ academics should be embedded in the records management system and supported by an appropriate records management framework. Additionally, institutions should develop and enforce policies regarding the retention and release of students’ academic records.

2.4 Importance of proper management of academic records

Academic records are invaluable resource to educational institutions when accurately recorded, maintained and secured. According to Bunawan et al. [14], the importance of academic records can becategorized into three key areas: “Application”, “Educational Development”, and “Solving Issues”. Also, Kane [15] outlines eight benefits of proper management of records as shown in Figure 2.

Fig.2. Benefits of proper records management.

2.5 Cybersecurity issues affecting academic data

Cyber security serves as a socio-technical measureaiming to secure computing resources from unauthorized accessandensure the integrity of information within in a computer system or transmittedacross networks [16].In today’s digital landscape, there is a rising accumulation of extensive andvaluable data containing information about schools and academic records of students [17]. Stored in files, these data contain valuable information about workers and students, making them attractive to cybercriminals [18]. Despite the obvious vulnerabilities in the cyberspace through which access is granted to those who need it,schools have not givendue attention to the security issues. As

a result, educational institutions havebecome targets of various kinds of attacks by cybercriminals to expose and gain undue access to sensitive information housed in records systems [19]. To effectively prevent such cyberattacks and recover incidents, establishing stronger communication channels between the IT directorate of schools and relevant stakeholders involved in academic data capture and utilization is imperative. The sophistication and multidimensionality of tactics employed by cybercriminals requires a comprehensive approach to managing these threats. The initial involves eliminating the threat source. Secondly, the vulnerabilities in the system must be identified and removed. Subsequent efforts then should be on mitigating the impact of the threat and restoring system's services.Given the time-consuming nature of these steps and the substantial labour-hours involved, enhancing the overall security system is crucial is imperative to minimizing the likelihood of a successful attack.

2.5.1 Forms of cybersecurity attacks on academic data

The attraction of academic data to cyberattackslies its rich content, particularly the wealth of student information stored within computing resources. Accessibility to student information,primarily through the internet, renders it susceptible to various kinds of cyber-attacks especially if the web application providing access to such information is poorly designed or have unguarded entry points[20]. The attacks on students' information can arise from diverse sources including seemingly benign programs that scan and log the keystrokes of users to steal login details. A divergence of viewpointsexists within the research and security community regarding information security. While specialists in the security community advocate forcentralized systems to facilitate monitoring and restrict access, researchers aim at enhancing the availability of academic data to students and to authorized users[20].

Despite the array of security solutions catering for the different viewpoints, concerns persist about the escalating number of cyber-attacks on academic data and associated breaches. Many of these attacks are orchestrated by organized crime groups colloquially known as "Drive-by hackers". The primary challenge in implementingpolicies for securing academic data lies in the independence of researchers. The independence in part, arise from the lack of alignment between researchers' needs and established cybersecurity protocols in academic institutions.Some argue that, mitigating cyber-attacks is either impractical or wasteful, emphasizing containment strategies that acknowledge the inevitability of such incidents [21]. Strategies focusing on ensuring data availability at all times are often prioritized.

The emergence of cloud computing applications introduces opportunities for instantaneous data recovery and backup efforts by security officials using advanced equipment and remote operations. The combined power of virtual machines and cloud computing presents a potential avenuefor effectively preventing cyber-attacks, enabling continuous monitoring, automating backup processes and facilitating the restoration of information and systems to theiroriginal states.

The common types of cyberattacks are [22]:

- Breaches of data (Exposure of private information to unauthorized users),
- security events (deliberate attacks at an institution of learning),
- violations of privacy (abuse of the privacy of consumers),
- Incidents involving phishing/skimming (financial crimes perpetuated by individuals),
- threats related to technology (hacking, malware and spyware),
- risks related to contents (granting access to unwholesome content),
- risk of information exposures (unauthorized exposures to personal information caused by phishing or through sharing information on social networking platforms)

3. ENHANCING THE SECURITY OF ACADEMIC RECORDS SYSTEMS

Numerous measures are currently in place to protect academic records systems from attacks and unauthorized access. In the following section, we will present suggestionsaimed at strengthening the security of students' academic records systems.

3.1 Implementing stronger authentication by academic records systems

Authentication based on Personal Identification Number (PIN) andpassword is common but gives weakdefenseagainst unauthorized entry in records systems. A PIN will typically be a short word code and so can easily be broken and deciphered. Thus, PIN-based authentications are susceptible to brute-force attacks. For instance,104-character combinations will be required to break a PIN made up of 4 digits.

A password may be longer but still will be as bad as a PIN especially if it is weak. A way forward is to devise and implement stronger authentication systems than the use of PINs and passwords. We suggest a credential-based system as a viable and better solution to authenticate users of academic records. In such authentication systems, a user is required to obtain a digitally signed credential from a legitimate provider. A user with such a credential is expected to show ownership of the credential in order to perform roles and operations in a records system. Authentication-based systems are less open to forgery and brute force attacks and as such are much more secure. The use of credential-based authentication systems will prevent unauthorized users from accessing the academic information of students in an academic records system.

3.2 Ensuring confidentiality in academic record systems

Like authentication, confidentiality measures are enforced in academic records systems to forestall sensitive student information from unauthorized access attempts. There are many ways to achieve confidentiality even by means of authentication measures such as the suggested credential-based scheme above. However, once an invader is able to gain entry into a record system, he or she is able to act at will. As a specific example, supposing the personal information of a student is transmitted via the internet or some internal network, to a target destination, an adversary who ordinarily does not have legitimate access privileges may eavesdrop on this information while it is in transit. To ensure the confidentiality of such information, better encryption schemes need to be applied.Traditional encryption schemes are not free from accidental or planned exposures. For instance, a legitimate holder of information may accidentally or deliberately share a confidential record with others who are not supposed to have custody of the such record. In that situation, the encryption scheme will be rendered ineffective. Therefore, in this article, a device-specific encryption schemeis proposed in which access to students' academic records is only possible from only certain devices. These encryption-enabled devices are assigned unique secret keys that will be the only required passcode to decrypt a specific academic record. Device owners will then be the only legitimate actors to access and use the records on their devices.

3.3 Ensuring prolonged availability of academic records system

Data availability is about a system's ability to allow timely and reliable access to and use of data; as well as the accessibility and continuity of information. Beyond gainingunauthorized access to academic records and making make use of information in there, many attackers aim at rendering a record system inactive and unavailable to serve legitimate users. This type of attack is commonly known as a denial of service (DoS) attack, and there are many methods of it with varying degrees of harm. The popular DoS method is designed to deliberately consume the system's resources by repeatedly forwarding data packets to it. In extremecases, a DoS attack may succeed in crashing the system and making it non-functional. Authors Gao et al. in [23]and Gao et al. in[24]have developed an efficient technique to deal with DoS attacks. Additionally, the guidelines below will be helpful in managing data availability:

- Regular backup of academic data
- Regular inventory of academic data;
- Securely dispose of or archive no-longer-relevant data or institutionally acquired devices following laid down institutional record retention policy and procedure
- Enforce the use of official institutional accounts and devices rather than personal ones.

3.4 Regulating and streamlining computer usage among major actors

Many of the security problems affectingacademic records systemscan be effectively addressed by ensuring acceptable and responsible user behaviour. Given that the majority of the computers that house academic records are based on the Windows operating system which inherently has certain security risks, it becomes imperative that authorized users of such Window-based systemshave and implement a scheduled programme to check the security of the operating system. Regular installation of security patches will additionally help to repair and extend the security potential of the underlying operating systems in use.

3.5 Regulate and enforce regular use and update of anti-virus programs

Viruses pose significant threats and canserve as means ofsecurity breaches in records systems. There are advanced virus detection systems designed to mitigate the operations of viruses. Therefore, operators of academic records systems should be obligated to install anti-virus software and conduct regular scansto cleanse computersagainstpotential viruses. Beyond installation, it is crucial that anti-virus programs are updated on a regular basis to reinforce the virus definition database against emerging viruses or strains of existing ones. The update process may be scheduled during non-disruptive peak working hours to prevent interferencewith in other academic functions.

3.6 Implementing key management technology

Weak passwords are vulnerable to simplebrute-forcemethods.To enhance the safety of students' data recorded on records systems that relies solely on passwords for security, users can employ key management technology to help them set and regularly change difficult-to-guess passwords. Such key management techniques can be tailored to set and enforcedistinct passwords for the different modules of a records system, granting access to data only when all the independent passwords are accurately entered. Regardless of the complexity of this security mechanism, it offers a certain level of protection to data stored in a computer system.

4. CONCLUSION

The security of students' academic records is a key concern that educational institutions must overcome. This paper explores the many kinds of security challenges faced by academic records systems and puts forthpractical measures to enhance the safer recording, storage and use of student data. Acknowledging the ever-evolving nature of information security, the suggested mechanisms put forth in this paper may losetheir efficacy in the future. Therefore, educational administrators and actors overseeing students' records must stay abreast with emerging security threats and regularly explore strategies to fortify and advance their students' records management systems.The emergence of wireless sensor network-based IoT technologies is a promisingavenue to address security exposures in students' academic records.

REFERENCE

[1] The Family Educational Rights and Privacy Act of 1974. 20 U.S.C. § 1232g, U.S. Department of Education. http://www.ed.gov/policy/gen/guid/fpco/index.html

[2] Frye, C. H. (1978). Tracking and Reporting School-Leaving Competencies: Keeping the Records, Displaying the Results. Northwest Regional Educational Lab., Portland, Oregon,

[3] Stewart, M. J., & Westgate, D. G. (2008). Information Management. Nelson, Canada, pp. 115-209Torton, A. (Ed) (1999). Managing business Archives. Butterworth: Heinemann Publishing.

[4] Somani, G. (2020). What is Student Record Management System and What are its Benefits? Retrieved from https://www.iitms.co.in/blog/student-record-management-system.html on 18th January, 2023.

[5] Shurville, S., Browne, H., & Whitaker, M. (2008). Employing Educational Technologists: A Call for Evidenced Change. In Hello! Where are you in the landscape of educational technology? Proceedings Ascilite Melbourne 2008.

[6] National Archives of Australia. (2002). Record keeping. Overview. National Archives of Australia Website: http://www.naa.gov.au/recordkeeping/overview/summay.html.

[7] Attwood, R., & Gill, J. (2008). Student numbers are at risk as UK demographics shift, Times Higher Education, http://www.timeshighereducation.co.uk/story.asp?storycode=406

[8] Azameti, M. S. K. & Adjei, E. (2013). Challenges in Academic Records Management in Tertiary Institutions in Ghana. *International Journal of Scientific Research in Education*, 6(3), 287-296

[9] Myler, E., & Broadbent, G., (2006). ISO 17700: Standard for Security. *Information Management Journal*, 40(6) pp. 43-52.

[10] Penn, I. A. (1983). Understanding the life cycle concept of records management Records Management Quarterly, 17(3), 5-8.

[11] Isa, A.M. (2009). Records management and the accountability of governance, PhD thesis, Humanities Advanced Technology and Information Institute, University of Glasgow, Glasgow, Scotland, viewed 15 May 2013, from http://www.theses.gla.ac.uk/1421

[12] Ngoepe, M. (2014). The role of records management as a tool to identify risks in the public sector in South Africa.*SA Journal of Information Management* 16(1). http://dx.doi.org/10.4102/sajim.v16i1.615.
[13] Ngoepe, M. (2011). Records management practices in the South African public sector Challenges, trends and issues, Lambert Academic Publishing, Saarbrücken.
[14] Bunawan, A. Kamal, J.I.A., Yunus, A. M., Abdul Kadir, M. R. & Hashim, H. (2016). Explaining the Importance: Proper Academic Records Management. Conference: *International Conference on Information Science, Technology, Management, Humanities & Business ITMAHuB*, 23, USA.
[15] Kane, M. (2022). Records Management in 2022: Why is it Important? Retrieved from https://www.imageapi.com/blog/importance-of-records-management, on January 28, 2022.
[16] Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology*, 3(3), 177-183.
[17] Goldsborough, R. (2016). Protecting yourself from ransomware. *Teacher Librarian*, 43(4), 70-71.
[18] Davis, D. (2018). Best practices for balancing technology use and safety in a modern school. In Society for Information Technology & Teacher Education International Conference (pp. 1026-1030). Washington, DC: Association for the Advancement of Computing in
[19] Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers & Security*, 73, 519-544.
[20] Alzighaibi, A.R. (2021). Cybersecurity Attacks on Academic Data and Personal Information and the Mediating Role of Education and Employment. *Journal of Computer and Communications*, 9, 77-90 https://www.scirp.org/journal/jcc
[21] Li, L., He, W., Xu, L., Ash, I., Anwar, M. & Yuan, X. (2019). Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behaviour. *International Journal of Information Management*, 45, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017
[22] Richardson, M.D., Lemoine, P.A., Stephens, W.E., & Waller, R.E. (2019). Educational Planning 2020, 9(2).
[23] Gao, Y., Mu, Y., & Susilo, W. (2005). A New Client Puzzle Scheme Against DoS/DDoS Attacks. *International Journal of Computer Science and Network Security (IJCSNS)*, Vol. 5 No. 10, pp.189–200,
[24] Gao, Y., Mu, Y., & Susilo, W. (2005). Preventing DoS Attacks with a New Client Puzzle Scheme. The AUUG'2005 Annual Conference, pp. 3–16.