UNIVERSITY OF CAPE COAST

NATURAL LANGUAGE PROCESSING (NLP) BASED PRIVACY PRESERVING ON TECHNOLOGY INTEGRATION USING SENTIMENT ANALYSIS: A CASE STUDY ON HIGHER EDUCATIONAL INSTITUTIONS' ELEARNING SYSTEMS.

EMMANUEL DERRY

2024

DERRY EMMANUEL

University of Cape Coast

UNIVERSITY OF CAPE COAST

NATURAL LANGUAGE PROCESSING (NLP) BASED PRIVACY PRESERVING ON TECHNOLOGY INTEGRATION USING SENTIMENT ANALYSIS: A CASE STUDY ON HIGHER EDUCATIONAL INSTITUTIONS' ELEARNING SYSTEMS.

By

EMMANUEL DERRY

Thesis submitted to the Department of Computer Science and Information Technology of the School of Physical Sciences, University of Cape Coast, in partial fulfilment of the requirements for the award of Master of Philosophy degree in Computer Science.

NOVEMBER, 2024

ABSTRACT

The COVID-19 pandemic significantly disrupted traditional education, accelerating the adoption of eLearning platforms in higher education. While eLearning offers numerous advantages, it introduces critical security and privacy concerns, especially in safeguarding students' data. This thesis explores the use of sentiment analysis to identify and address privacy issues from students' perspectives on eLearning platforms. A two-tiered model was developed by leveraging advanced Natural Language Processing (NLP) techniques, such as transformer-based architectures. The primary model performs sentiment analysis to classify user feedback as positive or negative, while a secondary privacy classifier identifies specific privacy concerns, including data breaches, identity theft, and location tracking, from negative sentiment responses.

Data for the study were collected from online repositories and augmented with web-scraped and manually annotated datasets. The methodology emphasizes a hierarchical approach to enhance computational efficiency and modularity. The findings provide actionable insights for eLearning management to enhance privacy-preserving measures, ultimately fostering a trustworthy digital learning environment. This research contributes to the intersection of educational technology, sentiment analysis, and privacy preservation, offering practical and theoretical implications for improving security in eLearning systems globally.

ACKNOWLEDGMENTS

Special thanks go to my family, whose love, sacrifices, and encouragement have been my constant source of strength. To my parents, Regina, Veronica and Lebron thank you for believing in me and supporting my dreams. To my siblings, Victoria, Mary, Josephine, Evans, and Elizabeth, thank you for your unwavering faith and understanding during challenging times.

I would like to express my deepest gratitude to my supervisors Dr Regina, Dr Alimatu-Saadia Yussif and Dr Abdul-Lateef Yussif, for their invaluable guidance, encouragement, and unwavering support throughout this research journey. Your insightful feedback and patience have been instrumental. I am deeply grateful to my colleagues and friends at the Department of Computer Science and Information Technology for creating an inspiring and collaborative environment. Your camaraderie, advice, and assistance, both academic and personal, have been a source of motivation and joy.

This thesis is a testament to the collective efforts of all the individuals who have supported me on this journey. Thank you.

TABLE OF CONTENT

TABLE OF FIGURES

CHAPTER ONE

INTRODUCTION

Educational sectors around the world were hardly affected by the breakout of the coronavirus pandemic in 2020, this together with technological advancement led to dramatic changes in educational delivery: heralding the adoption and usage of eLearning technologies. With the numerous benefits associated with this, many higher institutions have embraced this new change. (Kechaou et al., 2011) E-learning is defined as a form of education where students work on their own at home and interact with other students and teachers through chat rooms, electronic forums, videoconferencing, email, bulletin boards, and other computer-based communication tools. Among the positives, it has helped to broaden learning limits to encompass the outside world, and we receive new knowledge from others with whom we are unfamiliar; we reach out to others' networks to obtain the information we need: this is all enhanced by technological development and advancement specifically web 2.0 and eLearning technologies (Chang, 2021). That said, the eLearning and online courses have been popularized. However, moving from physical to online classrooms has not been without issues. Security remains a critical concern in online activities, particularly given the significant risks associated with hacking in today's environment (Kim, 2023). According to (Mujahid et al., 2021) numerous significant challenges present substantial risks to

e-learning compared to traditional classroom teaching methods. Understandably, security is essential to maintain users' trust in the online learning platform, as any risk could significantly impact students' views on the system's reliability and trustworthiness. (Chen & He, 2013). As per the literature, the current e-learning systems do not exploit the potential of learners' support to protect their privacy and to a larger extent resources on the eLearning system (Smrz, 2004). Therefore, it is relevant to study sentiment analysis on an eLearning platform's security and privacy issues in higher institutions. According to (Feng et al., 2020), the rapid advancement of artificial intelligence has led to the emergence of machine learning as a method for the automatic identification of academic emotions, marking a significant trend in development. In addition to providing useful information for examining how students behave in relation to a course, subject, or instructor, student sentiments and opinions can also be used to enhance institutions and policies(Kastrati et al., 2021). These opinions can equally be useful to eLearning managers to safeguard the security and privacy of learners in the eLearning platform.

1.1 Background to the Study

Digital transformation has become essential for higher institutions to constantly offer students teaching and learning regardless of their location through eLearning platforms. More individualized coursework and mixed learning approaches are now possible because to the development of online learning tools. Students may now learn, work at their own pace, and tailor their educational experiences to meet their objectives thanks to this trend. This significantly, provides

the learning community with a wide range of possibilities, including more flexible scheduling, access to educational programs, and qualifications (Yussiff et al., 2013). The Internet's rapid expansion and its capacity for immediate contact at any time and from any location have already completely changed people's lifestyles, organizations, and commercial endeavors. Universities will inevitably undergo fast change, and the old higher education model is facing tremendous strain from a society, culture, and technology that are always changing (Escotet, 2023). Therefore, in order to be competitive, current in every academic field, and appealing to students, institutions are going more digital and offering easily accessible remote learning platforms. The opportunities for advancing educational objectives appear endless with the increased availability of both traditional and online learning platforms. Higher education appears to be moving in the direction of more on-demand and accessible learning. Technology makes it possible for instructional resources to be delivered online and for information to be shared quickly, enabling learners to connect quickly and securelyAt the same time, the Internet has given us sophisticated tools and methods to engage in illegal conduct on the Internet where most eLearning technologies operate. Considering the dramatic rise in the use of online learning, security, and privacy issues have become more obvious and raised more issues (Slusky, 2020). All of the security hazards that come with using the Internet are also present when learning online (Chang, 2021). Lately, it is not uncommon to hear about identity theft and privacy violations, data leakage, location tracking, and online fraud that, in the absence of the Internet, would never have occurred (Yussiff et al., 2013). (Prinsloo et al., 2019) assert that

with the shift in the paradigm from traditional learning to online-based learning, user privacy is of great concern as the internet hosts perpetrators of various crimes. (He et al., 2015) postulate that to achieve a competitive advantage, listening to and understanding what consumer comment on the goods and services of rivals is often necessary. Hence, according to (Nasukawa & Yi, 2003) sentiment analysis's primary concerns include identifying how sentiment are conveyed in texts and if the opinions or phrases show favorable or unfavorable views about the subject, however, in this case eLearning systems. (Pathak et al., 2021) assert that making decisions promptly depend on individuals opinions, sentiment analysis is regarded one of the critical activities from a business perspective, and it is a highly demanded research domain. Similarly, it is important to understand the opinion of online learners on their privacy to be able to measure the level of trust from their perspective. (May & George, 2011) postulate that the participants' primary concerns are the protection of their sensitive personal information and the evaluation of the trustworthiness of the learning environments they use. Very little research has been done to pinpoint the task of classifying privacy issues on eLearning from the student's perspective. Concerning the framework, to conduct sentiment analysis and privacy classification, we initially, aimed to obtain the sentiment from response/inputs and then perform the classification at the input or sentence level. Most importantly, privacy-preserving algorithms will be used to secure the learner's perspectives before training the sentiment model and privacy classifier. However, in the existing security and privacy issues mitigation, most e-learning systems managers solely focus on providing security and privacy protection only from their

end (e.g. where the platform for communication is located). The users of the system are often ignored. In this vein, the granularity of the security and privacy protection should be rather large, yet it might not be precise enough to show the entire security and privacy protection process of the users on the e-learning platform. Based on this premise the user's perspective on their security and privacy could be obtained. This will help shape security and privacy-related issues on the eLearning platform and subsequently preserve individual privacy. (He et al., 2015) proposed a framework for gathering online consumer sentiment about a product's reputation. When compared to the traditional survey strategy, they discover that text mining approaches offer both a significantly lower cost and a greater amount of knowledge discovery from public opinion. Alternatively, (H. Lee et al., 2013) used a dataset gathered from MyStarbucksIdea, one of the most well-known online open innovation communities, was analyzed using both data mining and sentiment analysis approaches. Precisely, they used sentiment analysis to determine how each idea and comment gathered from the MyStarbucksIdea website was expressed. Using the trial results, they have developed a recommendation system that can assist businesses in sifting through a vast number of ideas to find potential innovations.

1.2 Statement of the Problem

(Chang, 2021; Onan, 2021) information and communication technologies and the internet, the application of Web 2.0, and Massive Open Online Courses

(MOOCs) have considerably affected many aspects, including education. The outbreak of the COVID-19 pandemic has significantly altered the way that education is delivered. As a response to this, the Internet and eLearning have been the optimal alternatives for face-to-face teaching and learning (M. M. Ali, 2021). eLearning can be defined as an online educational platform that provides educational resources to participants without distinctions based on gender, ethnicity, or location. eLearning platforms typically use traditional learning materials such as reading books, slide shows, brief video lectures, problem sets, live chat, and online tests. Largely eLearning supports the idea of lifetime individualized learning and continuous professional learning (Onan, 2021). Thereby, eLearning may comprise any educational programs that may be accessed and used online. These learning applications can be made for self-directed, cooperative, or collaborative learning. Specifically, with multi-user eLearning platforms, pertinent activities such as instruction, learning, and organizing, are represented by distinct roles and must be distinguished: the learner, the tutor, the mentor, and the administrators. Personal information must be shared for the aforementioned roles to interact. (Khurana et al., 2023). (Aïmeur et al., 2007) identifies major components of a typical eLearning system including the Tutor Environment, Learner Environment, Data Storage, and System Manager. According to (Alier et al., 2020) the stakes are considerably higher when it comes to information technologies in education. In the current scenario, the educational institution has no control over the student's data. This data is sought after by the newly researched and produced learning technologies to build the ideal learning

environment, where teachers and students are subtly persuaded to accomplish what they are asked to do by means of incentive systems and digital environments. However, in any case, (Borcea-Pfitzmann & Stange, 2007) postulate that there is always a trade-off between privacy and opportunities while acting in an informational society. That notwithstanding it is mandatory to offer privacy as possible to the individuals using the eLearning System.

(Ivanova et al., 2022) discussion privacy in eLearning, considering questions related to data management, informed consent, and the construction of intelligent eLearning environments. Importantly, it points out the need for privacy preservation in eLearning, considering the implemwntation of Learning Analytics (LA) based softwares and the application of contemporary privacy-preserving technologies. Given this, emphasis was made on the need for a balanced approach to protect student privacy. According to (Kechaou et al., 2011) Conducted a comprehensive survey of users' thoughts and opinions is one of the most important responsibilities of eLearning administration, to meet their demands and specifications as effectively as feasible. A method to find positive and negative sentiments about particular topics (such companies and their goods) within textual data provides a wealth of options for different applications. Such techniques according to (Nasukawa & Yi, 2003) would offer strong capabilities for marketing analysis, competition analysis, and risk management by detecting negative rumors. Ensuring data privacy in eLearning is a difficult problem in our open and shared virtual world. Therefore, a holistic approach is needed to mitigate the problem. Thus, both the management and the student have a role to play. (Nasukawa & Yi,

2003) asserts the need for an innate desire to identify and evaluate favorability in online documents, such as news stories, chat forums, and Web pages, rather than creating unique surveys using questionnaires that are laborious, time-consuming, and difficult to process and understand. Nonetheless, analyzing positive and negative viewpoints is a difficult process that calls for high intelligence and a thorough comprehension of the textual context, utilizing both linguistic and topic expertise as well as common sense. Particularly during the COVID-19 pandemic, when the majority of educational institutions switched from traditional in-person instruction to online learning, the value and popularity of student evaluations have also grown recently (Kastrati et al., 2021). Unlike in-person teaching-learning environments, where privacy might not be an issue, online learning environments require the collection of personal information to personalize the user's learning experience of each learner this perspective presents privacy and security issues for the learners and the eLearning platform managers to deal with. Relying on asynchronous text-based communication may alleviate the level of privacy issues (Dolianiti et al., 2018). Therefore, the learners need to be involved to mitigate any privacy issues.

According to (He et al., 2015) the current Massive Open Online Courses (MOOC) do not have frameworks that provide benchmarks that allow the platforms to compare learners' sentiments on security and privacy to understand where privacy preservations must be improved easily. As many learners do not clearly show nor express or state their dissatisfaction regarding their privacy issues in some contexts, hence, need to predict it from the reponses text data. This text data

contains the reviews of the learners, as these reviews are often extensive in quantities, it is laborious, or even impossible, for eLearning management to read all of them and identify their orientations (Kechaou et al., 2011). As we identify sentiment behavior from students' discussion forums, we can evaluate the learning environment's efficacy in making improvements to student's learning process, the teaching experience of tutors, and the institutional strategic perspective of the university (Gkontzis et al., 2017). Early detection of customer complaints and service issues lowers the possibility of defective products being widely distributed improving promotional strategies (Kechaou et al., 2011). That said, sentiment analysis can play an important role in enhancing the eLearning management security strategies to protect the learner's personal information and address other privacy issues accordingly on the eLearning platform. From a technology standpoint, technological methods continue to be crucial in addressing security and privacy concerns. Thus, Natural Language Processing a subcategory of Artificial Intelligence can help provide solutions to security and privacy issues. Similarly, student's security and privacy can be improved from the student's perspective expressed in textual form. (Waheeb et al., 2022) observed that the subjective nature of textual data from students who use the E-learning platform can be used to determine attitudes, sentiments, and opinions while using the online platform for learning. The algorithmic identification and investigation of viewpoints, attitudes, emotions, and subjectivities in text is known as sentiment analysis (He et al., 2015). Also, it can be defined as a branch of affective computing that calls for addressing a number of subtasks in natural language processing, such as subjectivity detection,

concept extraction, named entity recognition, and sarcasm detection (Y. Li et al., 2017). It consists of topic-specific feature term extraction, sentiment extraction, and association via relationship analysis, and it operates by obtaining sentiments about a certain topic. (Khurana et al., 2023). The document level, phrase level, and aspect level are the three general levels at which sentiment analysis can be carried out. By examining the entire document, sentiment analysis at the document level seeks to determine user sentiments. Sentence-level analysis is more detailed since it focuses on determining the polarity of individual sentences rather than the document as a whole. Finding features or characteristics mentioned in reviews and categorizing user sentiment on these features are the main goals of aspect-level sentiment analysis. (Kastrati et al., 2021).

In business settings, sentiment analysis is used to study and examine how people feel about services, products, mandates, and organizations (Pathak et al., 2021). (Onan, 2021) used sentiment analysis on educational data to get input on resources and learning materials, which provided helpful information to improve the calibre of instructional materials and determine how pupils learn. Although data mining, text analysis, and sentiment analysis techniques are frequently adopted to conduct social media analytics (He et al., 2015), these techniques can also be adapted to mine the sentiments of learners regarding their privacy on an eLearning platform. Depending on the above premise, this thesis proposes a method for sentiment classification based on privacy to categorize learners' opinions about their privacy on the eLearning platform into positive and negative in a way to improve and provide prompt awareness of any privacy issues that may arise. And

subsequently, provide awareness of the most prevalent privacy issues that the learners encounter. From the learners' perspective, several papers have used sentiment analysis to look into the relationship between students' sentiments and dropout rates in Massive Open Online Courses (MOOCs), as well as the relationship between attitude and performance with learners' sentiments. To the best of our knowledge, however, the body of literature is used to establish the status of evidence lacks a sentiment analysis of students' feedback regarding their privacy and security issues on the adoption and usage of eLearning fueled by the outbreak of the coronavirus and technological advancements. This approach will allow the people in management eLearning to identify any possible problems especially security and privacy issues that might be encountered and need to promptly resolve such problems and further, foster robust privacy preservation implementation.

1.3 Purpose of the Study

Privacy in the digital space has always been of great concern. This situation of friction could be solved with the use of the underlying technology of Natural Language Processing (NLP). Where the learner's opinions are mined and feedback is served to the managers of the eLearning system to further foster robust privacy preservation implementation. (Ivanova et al., 2022) suggest the utilization of machine learning to support decision-making regarding suitable data privacy

preservation models. This study aims to leverage sentiment analysis to address security and privacy issues on eLearning systems from the perspective of learners. Further, an in-depth understanding of the privacy issues and challenges faced by students and faculty when using eLearning technologies. And subsequently, build a sentiment and privacy classifier model that will help make recommendations to upgrade the privacy-preserving metrics within the eLearning platform in the selected higher educational institutions in Ghana.

1.4 Research Objectives/Questions

To plan this study, we came up with research questions that were pertinent to our goals. Defining research questions is the most crucial aspect of this thesis study because they influenced the design of the research procedure. The following research questions were developed to achieve these goals:

1. How can sentiment analysis be effectively applied to identify prevalent privacy concerns expressed by students using eLearning platforms in higher educational institutions?
2. What specific privacy issues are commonly raised by students in negative sentiment responses, and how can these issues be addressed through effective privacy preservation measures?
3. How can higher educational institutions leverage sentiment analysis and privacy classification models to proactively identify and mitigate privacy issues within their eLearning environments?

The research objectives accompanying the questions are below:

1. Develop a robust sentiment analysis model capable of accurately classifying user responses as positive, or negative in the context of privacy concerns on eLearning platforms.
2. Train a privacy classifier model to identify specific privacy concerns within negative sentiment responses, focusing on issues such as data collection, data breaches, Identity theft, and Location Tracking.

3. Develop recommendations for higher educational institutions to address the identified privacy concerns, including implementing appropriate privacy preservation measures and fostering a culture of responsible data handling.

1.5 Significance of the Study

In this study, we present a sentiment and privacy classifier model with benchmarks that can be used to glean the eLearning environment in higher institutions. This will enhance and identify specific actionable areas in which the eLearning environment is leading and lagging regarding the security and privacy of the learner. This will further build learners' trustworthiness of the system. This approach will offer higher educational institutions and decision-makers a way to track and quantify students' satisfaction concerning security and privacy on the eLearning platforms. In addition, the system could help to eLearning management officials determine the development and high points of concern for the learner's security and privacy in space and time, which will enable the implementation of

appropriate preventive actions to mitigate any security breaches and ultimately possibly prevent their occurrences. More to that it will also help authorities in advocating security and privacy awareness in higher institutions and promoting social responsibility in cyberspace. In furtherance, this research will provide practical recommendations considering the results of the study. The recommendations will be specific to the selected higher institutions but may also have broader implications for eLearning practices and privacy considerations in other higher educational institutions. Additionally, the significance of this study holds not only for the selected higher institutions but also for commercial providers such as the Massive Open Online Courses. The study may add to the corpus of information in the fields of educational technology, privacy, and sentiment analysis, potentially leading to further research opportunities and publications. The security and privacy of the data and the preservation of the privacy of the students are those that are considered most important to this thesis. And sentiment analysis could accomplish this by examining students' textual feedback traces the opinion of their privacy issues in the eLearning environment. According to (Ortigosa et al., 2014) the students' sentiments towards a course can serve as feedback for teachers, especially in the case of online learning. On the flip side, the sentiment of the students on their privacy would equally serve as feedback for the eLearning management to further enhance privacy-preserving security metrics.

1.6 Delimitation

The scope is broad but concentrated on the unique setting of these selected higher institutions in Ghana: the University of Cape Coast, the University of Energy and Natural Resources, and Kwame Nkrumah University of Science and Technology. The context of the study is using Natural Language Processing to build a sentiment and privacy classifier model on the privacy issues of learners in the eLearning platform of the selected higher institutions. Although, there might be other workers in those higher institutions using the eLearning systems the focus of this research is geared toward only the students' feedback, perceptions, or opinions regarding their privacy on the eLearning platform.

1.7 Limitation

Among the elements that might improve the model's performance were word embeddings that were trained on datasets specific to a domain instead of other domain data. To the best of my knowledge, there are no word embeddings purposely created to represent the domain of security and privacy. Sentiment analysis heavily relies on domain-specific knowledge because every area has unique scenarios that are both desirable and unattractive. (Dolianiti et al., 2018). Again, other the sample size and the space horizon under analysis are the study's limitations. Moreover, sentiment analysis covers both speech and textual data, nonetheless, this study focuses on textual data. Another limitation to this study will occur when the learners express their opinions , irony and sarcasm can occasionally

be understood. oppositely by humans, and so this model may fail to deal with such opinions and present undesirable outcomes.

1.8 Definition of terms

1. **E-learning**: Clarifying what is meant by E-learning, which could involve defining online educational platforms, virtual classrooms, or any other specific aspects related to electronic learning.

2. **Sentiment Analysis**: Providing a clear definition of sentiment analysis, including examining and understanding sentiments, viewpoints, and attitudes that are conveyed through textual data.

3. **Privacy Issues**: Privacy issues encompass challenges or problems related to the defense of individuals' personal information. In the context of this thesis, privacy issues refer to specific instances or aspects where the confidentiality of data in E-learning may be compromised.

1.9 Organization of the Study

There are five chapters in this work. In the first chapter, the study's background, problem statement, purpose, research questions, significance, scope, and organization are all covered. Chapter 2 “Literature Review” covers a review of

research work on privacy in E-learning, Sentiment Analysis, machine learning, and the various initiatives taken by previous researchers in the field of sentiment analysis. Chapter 3 “Research Methods” encompasses the methodology's step-by-step process is depicted, along with the techniques, algorithms, and data status in each stage in this chapter. It starts with data collection from the students at the various selected higher institutions. The dataset is then cleaned using a number of preprocessing techniques. A detailed description of the research that was done is given in Chapter 4 “Discussion” highlighting a detailed analysis of the conducted survey. The latter section of the study Chapter 5 summarizes the key conclusions and outlines some recommendations for the future.

In summary, the background is given in this chapter which highlighted the transformative impact of the COVID-19 pandemic on educational deliveries, leading to a surge in eLearning adoption. We outlined the purpose of the study, which aimed to leverage sentiment analysis to identify and address security and privacy issues from the viewpoint of students in higher educational institutions. The research objectives and questions were formulated to guide the study, focusing on understanding privacy issues, fostering a culture of responsible data handling, and proposing recommendations for enhancing privacy and technology integration. The significance of the study was underscored, emphasizing its potential to enhance learners' trust in eLearning platforms, provide actionable insights for decision-makers and add to the corpus of information in educational technology and privacy.

CHAPTER TWO

2.1 Introduction

In the previous Chapter, we explored the background of the study, emphasizing the growing importance of eLearning and the accompanying security and privacy concerns. In this new chapter, we delve deeper into the literature reviewed in Chapter 1, highlighting key themes, findings, and gaps identified. The transformative effect of the COVID-19 pandemic on education underscored the urgency of adopting eLearning technologies. According to some estimates reported by (Slusky, 2020) the worldwide eLearning market has surpassed the $100 billion mark. Moreover, the transformative impact of the COVID-19 pandemic on education underscored the urgency of adopting eLearning technologies to replace classroom instruction in colleges and schools, and eLearning technology use grew rapidly.. However, this transition brought forth significant challenges, particularly in ensuring the security and privacy of learners' data in online environments. Although e-learning's benefits have received a lot of attention, security and privacy concerns must be considered because this move away from traditional methods may result in security and privacy concerns (Qureshi et al., 2012). Users' view of the possibility that the service provider they share their data with will take adequate precautions to shield it from misuse, such as unwanted disclosure or unauthorized use, is known as perceived privacy protection. (Mehta et al., 2022). Therefore, emphasis must be placed on understanding learners' perspectives on privacy issues

through sentiment analysis, which can provide valuable insights for improving eLearning environments. Higher educational institutions face specific privacy challenges in their e-learning systems. These challenges include issues related to data collection, use, and distribution, as well as ensuring transparency, information security, accountability, and data privacy (X. Li & Pei, 2023). The main privacy challenge faced by higher educational institutions in their e-learning systems is ensuring data privacy. This is particularly important because e-learning systems often gather and preserve a lot of private information, especially sensitive data about students. Information on customers can be gathered and stored thanks to the internet and all of its offerings (Azemović, 2012). Information systems deal with increasingly large amounts of personal data in essential services such as eLearning systems. (Lin et al., 2004) identifies administrations, courseware authoring, course content delivery, synchronized communication, multimedia lecturing, and student performance assessment as some catalogued functions of eLearning systems. According to (Basu et al., 2021) any business that gathers or keeps personally identifiable information must now protect the privacy of sensitive client data.

2.2 Background and Context

According to (Pekárek & Pötzsch, 2009), the absence of unjustifiable limitations on the process of constructing one's identity is known as privacy. Strong precautions must be taken to protect users' personal information on various systems, particularly eLearning systems, and to reduce information misuse since the availability of personal information in the hands of unauthorized parties may result in such limitations. The design, architecture, business model, and operation of e-

learning have changed over time due to these advances, which include interoperability standards for educational resources, software as a service, and cloud computing. Consequently, according to (Alier et al., 2020), there are institutions in 2020 where not a single piece of student data is kept on university-owned servers. The metadata and learner data have gotten out of the institution's hands. Additionally, this greatly increases the possibility of problems with student data privacy. Security and privacy problems have grown in prominence and raised more awareness in light of the rapid shift to online learning (Slusky, 2020). Stakeholders who are actively engaged in online instruction are concerned about the security of e-learning technologies. That said, according to (Hasan et al., 2014) an essential component of distributed, interactive, and open learning systems is security. Although information technology is increasingly employed to improve online learning, especially with new technologies, it frequently falls short of addressing the security issues associated with online education (Slusky, 2020). The architecture and content for the eLearning system have been developed with a great deal of work, however, the system's security has received very little attention (Kritzinger, 2006) (R. Ali & Zafar, 2017), (Bhatia & Maitra, 2018). Nevertheless, information system security is currently a significant issue for all businesses. It is important to remember that an efficient e-learning environment is dependent on on participants who recognize the value of security and act appropriately (R. Ali & Zafar, 2017). Research from a variety of e-learning providers shows that a user's study habits, platform access points, and content accessibility are all related to privacy problems (Majeed et al., 2016). An eLearning system should be adequate

to safeguard the learner's personal information and should not jeopardize any threats. (Aldheleai et al., 2015). Moreover, (Reidenberg & Schaub, 2018) argues that it will be necessary to create privacy protections using technology. Hence sentiment analysis from the perspective of the learners can be a useful technological tool to safeguard users' privacy by providing feedback to the management of the eLearning system regarding their security. When systems are in place to foster that privacy and trust, students will feel more comfortable engaging and working together. For an eLearning environment to function, students' requirement for security must exist. (Martinelli et al., 2020) asserts that Privacy and Data Protection (PDP) is widely acknowledged to provide a leading edge in academic, legal, regulatory, and technological advancement. When handling personal data and system credentials of an individual, the idea of privacy preservation maintains a high degree of seclusion. Accordingly, (Azemović, 2012) observed that for consumers of contemporary information systems, maintaining their privacy is crucial. According to (Ackerman et al., 1999) numerous studies carried out globally over the past 10 years have regularly revealed high levels of privacy concern. Recent privacy scandals and data breaches, like Cambridge Analytica and many others have probably spurred debate, more targeted policymaking, and additional study. (Silva et al., 2020). Previous studies suggest that privacy is intricate, diverse, and heavily dependent on circumstance. People have different views on privacy, and they frequently claim to be worried about privacy yet act in ways that betray this concern (Besmer et al., 2020). However, (Lin et al., 2004) also asserts relatively little research has been done on how to provide users with security and privacy

when engaging in educational activities. As a result, when students are learning in this setting, fundamental security requirements including availability, confidentiality, and integrity must be guaranteed (Raitman et al., 2005). Even with these safeguards in place, hackers can still access user data on the eLearning system by using a variety of highly sophisticated developed resources. The recipients are always the pupils or learners, though. To enable the systems to be adjusted as needed, a technologically sophisticated method of alerting management to privacy violations must exist.

The concept of a comprehensive strategy for protecting students' privacy on e-learning platforms is presented in this thesis through sentiment analysis and privacy issues classification. According to (AL-Rubaiee et al., 2016), at least 54% of online student comments were more thorough and educational than the written comments that are often left on paper. This highlights how crucial it is to pay closer attention to comments made online. The drawback is that analyzing comments made online takes more time and necessitates the use of an automated feedback system for collection and processing. The goal of gathering and examining as much user activity data as possible to have the power to shape users' behavior is not unique to the typical suspects in large corporations (Alier et al., 2020). Moreover, the precise goal is found in the major innovations and research trends in education, such as proctoring, gamification, adaptive learning, and learning analytics. The level of dependability and security required for an efficient eLearning system is not offered by the Internet. While this is true, there are methods to get around a lot of issues and still maintain a reasonable level of security.

The consequences of failing to protect personal and academic data can be severe, both legally and reputationally (Roussos et al., 2023). A data breach can cost a university money, more so, it can also harm the institution's brand and lose the confidence of its constituents, who include donors, employees, and students. According to (Borcea et al., 2006), users are becoming more aware of privacy risks in other application domains, such as e-commerce. This hasn't been the case in the eLearning sector up until now. However, privacy issues will eventually show up as major barriers to the acceptance for eLearning systems(Reidenberg & Schaub, 2018) argued for the need to demonstrate the efficacy of learning systems while respecting privacy and how to build accountability and oversight into learning technologies. A few privacy-preserving strategies were developed and presented to the research community since privacy is quickly emerging as one of the main issues with open systems, like the Internet. The majority of these studies are carried out in-depth in the fields of software engineering often at the expense of user input to notify management about security vulnerabilities that they may have come across or heard about. (Yong, 2011). (Alier et al., 2020) postulate, it is clear that the current culture in the field that researches subjects like learning analytics, gamification, adaptive learning, proctoring, and—too horrifying for the authors—emotional analysis of the students does not think that using the students' personal information is unethical. There exist undoubtedly incentives in place to collect as much information as possible on students' usage of learning resources.

2.3 Privacy concerns in higher educational elearning systems

As information-sharing technologies continue to evolve, protecting users' digital privacy has emerged as a critical concern. (Mehdy & Mehrpouyan, 2020). Informational privacy is defined as the right to manage one's data and is intimately linked to several personal spheres. Informational privacy was the foundation upon which some scholars built the notion of privacy in e-learning (Chou & Chen, 2016). The phrases privacy, informational privacy, and data protection shall be used interchangeably in subsequent discussions. We must take into consideration learners' privacy concerns even as we promote open knowledge sharing in an online learning environment. The inherent privacy hazards associated with online education may include location monitoring, identity theft, data leaks, impersonation, insufficient authentication, and many others. (Chang, 2021) claims that ensuring students' privacy safeguards a secure learning environment. Online education also needs to take into account the inherent privacy hazards associated with it. Higher education's use of eLearning has resulted in new demands for institutional planning, infrastructure, logistics, regulations, information usage, and security issues due to its evolution and the new approach to its objective (R. Ali & Zafar, 2017). The vast number of potential information security risks associated with Internet use is making it increasingly challenging to implement information security safeguards. (Derawi, 2014; Hilmi & Mustapha, 2022). The danger increases with the complexity of online learning systems' features and functionalities (Chen & He, 2013). Regardless, information must be safeguarded to prevent its availability, confidentiality, and integrity from being compromised.

(Derawi, 2014). Involving all parties as well as those in the institution's immediate vicinity, however, could make it easier to adopt a thorough and successful security and privacy policy. A comprehensive solution is necessary to handle the multiple privacy problems in higher education eLearning systems(Chou & Chen, 2016) postulate that a substantial amount of e-commerce research has discovered that consumers are more inclined to make purchases online when they are in a secure e-commerce environment. From this perspective, it is ideal to say that the safety of eLearning environment will help increase learners' willingness to patronize eLearning platforms. Accordingly, (Raitman et al., 2005) asserts that a protecting students' privacy ensures a safe learning environment. Nevertheless, learners' inclination to use eLearning platform services may suffer if they believe their privacy is in jeopardy. As a result, eLearning loses its effectiveness since users are too terrified to use the materials meant to aid in their learning in the first place. (Slade et al., 2019) after performing sentiment analysis on the terms and conditions of Massive Open Online Courses reported that an overwhelming sentiment was found in their qualitative analysis and that what is really at stake is the protection of the rights of the provider rather than the user. In addition, (C. B. Lee et al., 2022) carried out research to learn about Chinese SNS users' attitudes and views on online privacy by collecting and examining their comments regarding the Facebook-Cambridge Analytica privacy breach. According to the information discovered, consumers believed they had no say in how businesses gathered and used their data. Additionally, a few of responses claimed that internet privacy does not exist. This increased awareness presents an opportunity for individuals, companies, and

policymakers to engage in meaningful conversations and take proactive steps toward enhancing online privacy protections. By acknowledging the concerns raised by users and working collaboratively to address them, High Institutions can strive towards a future where learners feel empowered and confident in the eLearning platforms, ensuring that privacy remains a fundamental right. (Saura et al., 2021) conducted sentiment analysis on 67,206 tweets including the keywords #Industry40, #Privacy, and #Security. Using the sentiments stated in the tweets as a guide, the Latent Dirichlet Allocation (LDA) topic-modeling technique partitions the database into themes. They came to the conclusion that strategies that include machine learning as a key technology are the most successful. Regardless whether a person learns in an online or offline setting, privacy is a basic right, according to research findings reported by (Majeed et al., 2016). Therefore, it is difficult to impose all-inclusivity to privacy mitigation unless a comprehensive strategy including all stakeholders—users, learning management, etc.—is adopted. (Hilmi & Mustapha, 2022), conducted a study that looked at how students viewed their eLearning portal's security. A total of 497 students responded to a survey questionnaire. Frequency analysis was used to display the respondent's profile. The respondent's perceptions are often very positive toward the security in their Learning Management System (LMS). The study takes a more complete approach to perceived security, encompassing not just technical elements like confidentiality and authentication but also a student's overall feeling of safety and wellbeing on their learning management system (LMS). According to (Al-Hail et al., 2023), learners feel worried about using online learning because of privacy and ethical

issues. Although, their terms and conditions spell out the purpose and use of the data, a study by (Prinsloo et al., 2019) suggests that MOOCs are much more interested in protecting their interest, not the users or clients.(Azemović, 2012) conducted a survey on privacy preservation using the Hippocratic databases (HDB) concept, although the HDB eLearning prototype successfully satisfied all of the requirements, which have been empirically validated, according to the measured outcomes of access control, it still does not allow the students or learners to provide some sort of relevant information such as privacy breach that might be necessary for further privacy preservation implementation.

Further in works by (Hasan et al., 2014) they used multi-agent technology to secure eLearning applications. And described the use case to ensure Privacy and integrity via 3 use case paths: Try to compromise the message integrity of the system. Try to compromise the integrity of the user's message. An attempt to compromise the integrity of the assessment. In all these cases the learner's perspective cannot be gleaned which might be useful to the eLearning management for the effect of privacy-preserving policy implementations. (Besmer et al., 2020) in their study used used supervised machine learning to distinguish between reviews that are about privacy and those that are not. They then used natural language processing sentiment analysis to compare differences between the groups. Accordingly, (Pekárek & Pötzsch, 2009) emphasized the necessity of addressing differing views of privacy in educational data analytics. After, the research showed that there are differences in students' willingness to agree to learning analytics. (Ahmed et al., 2011) in their study assert that the possibility of

technical strategies can be used to combat security threats: digital signature information security mechanisms, token-based information security mechanisms, biometrics information security, SMS information security, and access control list (ACL) mechanisms. Contrary to that, it appeared in research conducted by (Pekárek & Pötzsch, 2009), that the observed disparity between expressed data protection attitudes and actual behavior already limits the potential of such technical measures above to absolve all privacy issues. Due to the focus on students' privacy concerns in learning analytics, models like the Students' Privacy Concerns in Learning Analytics model have been developed and validated (SPICE) (Mutimukwe et al., 2022).

Moreover, research has delved into views of students regarding privacy in courses with greater technology, highlighting the need to understand the balance between inclusion and potential privacy infringement (Blackmon & Major, 2023). Similarly, using tracking systems in eLearning has raised privacy concerns, necessitating a closer understanding of the potential privacy threats posed by such systems (May & George, 2011). Again, the shift to exams that were e-proctored during the epidemic have provided insight into how students view privacy as well as a number of environmental and psychological aspects, underscoring the importance of recognizing and resolving privacy issues in eLearning platforms (Kharbat & Abu Daabes, 2021). Efforts to enhance the privacy of eLearning systems have explored the use of aliases and anonymity to implement privacy preservation measures, offering potential strategies to safeguard student privacy (Yong, 2008). Ideally, they don't provide a complete solution. To truly empower

users and build trust, future advancements need to address user perceptions of security and offer more comprehensive safeguards.

2.4 Nlp-based privacy preservation.

It is crucial to consider the many approaches and difficulties involved in developing and evaluating technologies in Natural Language Processing (NLP) that protect privacy and to apply it in privacy preservation in eLearning systems (Mahendran et al., 2021). NLP methods can be used for entity detection and text classification., and sentiment analysis in educational domains, such as eLearning systems (Basu et al., 2021). There have been more and more research using NLP approaches to solve industrial issues (Baker et al., 2020; Moon et al., 2022). In (S. Xu et al., 2020), Used deep learning techniques and BERT characteristics, a predictive model is suggested to determine the helpfulness scores of customer reviews. As the authors explain, it is logical to expand the use of BERT to insurance data (A. Wang et al., 2018) already highlight BERT's potential as a tool for analyzing insurance data. Recently, researchers have looked into using BERT-based NLP approaches for severity modelling through loss prediction and portfolio classification. (S. Xu et al., 2022). This study tends to leverage sentiment analysis and text classification to determine the emotions of the learners concerning their privacy and the most prevalent privacy issues in eLearning systems. (M. M. Ali, 2021) used machine learning (ML) and natural language processing (NLP) techniques to do sentiment analysis and emotion mining. They studied negative emotions, using a range of classification techniques, and used the NRC Word-Emotion Lexicon and Information Gain as a filtering technique. Their model's

Support Vector Machine (SVM) classifier yielded an 89.6% success rate. (Khan et al., 2022) used a hybrid CNN-LSTM model, which incorporates several word embedding techniques and machine learning classifiers, to properly categorize text into negative, positive, or neutral feelings. They conducted a sentiment analysis on Roman Urdu material from social media. Following this study, the Transformers (BERT) model's cutting-edge bidirectional encoder will be used to train both the sentiment and privacy classifier models. (M. M. Ali, 2021) provided a thorough Sentiment Analysis (SA) and Emotion Mining approach in their study, using methods from natural language processing (NLP) and machine learning (ML). To assess the sentiment analysis performance, many categorization methods were used. Since the Support Vector Machine (SVM) outperformed the other methods in terms of accuracy, precision, and recall, they decided to adopt it as their primary classification algorithm. Using deep learning and ensemble learning paradigms, (Onan, 2021) offered a system for classifying reviews of Massive Open Online Courses (MOOCs) based on sentiment. The study's conclusion shows that deep learning-based models/architecture were far better than ensemble. Additionally, supervised methods using GloVe word-embedding representation in long short-term memory networks were proposed by (Pennington et al., 2014), outperforming them with a high classification accuracy of 95.8%. To this end, the (Onan, 2021) informed our decision to explore deep learning-based architecture such as BERT in building both the sentiment model and the privacy classifier model.

2.5 Applications of sentiment analysis in privacy preservation

With better performance than conventional machine learning techniques, deep learning has become a potent technique for sentiment analysis. (L. Zhang et al., 2018). Numerous sentiment analysis tasks have demonstrated the effectiveness of Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), especially Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) variants. (Joseph et al., 2022). These deep-learning models can automatically discover intricate semantic representations from text data without extensive feature engineering (Tang et al., 2015). Word embedding techniques such as GloVe, fastText, and word2vec, combined with CNNs, have been applied effectively to sentiment analysis of Twitter messages (Onan, 2019). Deep learning approaches have advanced the latest developments in sentiment classification, sentiment extraction, and sentiment lexicon learning (Tang et al., 2015). However, challenges remain, including handling large-scale datasets and addressing domain-specific nuances in sentiment expression (L. Zhang et al., 2018). (Qazi et al., 2017) Sentiment analysis is one of those "suitcase" research problems that involves solving several NLP subtasks, such as entity recognition, aspect extraction, subjectivity detection, and sarcasm detection. To get insightful information, the primary objective has been to extract views on entities. (Kechaou et al., 2011) Sentiment analysis for e-learning involves utilizing a process for autonomous text analysis to identify and extract opinions from the wide range of sentiments expressed in e-learning platforms. Learners describe or discuss their viewpoints and assessments regarding the services offered and privacy-protecting security

measures. In (Colace et al., 2014) research, sentiment analysis was applied to student talks gathered from the chat and forum on Moodle in a course that incorporated mixed learning. The findings indicated a generally favourable trend in the students' attitudes during the course, as the instructor modified their methods of instruction to better suit the needs of the students by providing additional activities and examples. In the work of (Chaplot et al., 2015), three Massive Open Online Courses (MOOC) platforms were considered a lexicon-based strategy for sentiment categorization of student contributions relating to preset subjects (e.g., course, lecture, assignment). Additionally, (He et al., 2015) provided a system for gathering online consumer sentiment on product reputation. When compared to the traditional survey strategy, they discover that text mining approaches offer both a significantly lower cost and improved information identified from public opinion. As an alternative, (H. Lee et al., 2013) examined a dataset gathered from MyStarbucksIdea, one of the most well-known online open innovation groups, using sentiment analysis and data mining approaches. They specifically employed sentiment analysis to determine the sentiment present in every suggestion and remark gathered from the MyStarbucksIdea website. They have developed a suggestion system that may assist businesses in identifying potential innovative ideas from a vast pool of ideas with the usage of the testing outcomes. The most common privacy concerns that can arise in eLearning systems have not yet been investigated using this innovative method.

(Onan, 2021) used sentiment analysis on data related to education to gather information on learning materials and content. This yielded insightful information

that helped improve the materials' quality and pinpoint students' learning habits. Also, (Xiao et al., 2018) developed a novel sentiment analysis on Facebook, focusing on classifying text messages according to their opinion being either positive, neutral, or negative. This strategy combines machine learning and lexical-based approaches to obtain excellent sentiment classification accuracy. To identify changes, the program records each student's attitude toward the course and compares it to their typical behaviour. By utilizing sentiment analysis and privacy issues, the article's technique aims to improve mobile personalized service (MPS). Although there is much research on sentiment analysis, with a primary emphasis on product evaluations, online course evaluation (Onan, 2021), and many others. (Alatrista-Salas et al., 2019) introduced a sentiment analysis methodology utilizing Bloom filters that is sensitive to privacy. Before training the model, textual data is preprocessed using Bloom filters, and the method is assessed using four supervised learning algorithms on three corpora. Metrics including calculation time, accuracy, Disclosure Risk (DR), and Information Loss (IL) are used in the study to assess performance. Findings show that the privacy method has no discernible impact on algorithmic performance, guaranteeing efficient privacy-aware sentiment analysis. A sentiment analysis-based method for categorizing students' feelings about e-learning materials is presented by (Mandal et al., 2017). The suggested sentiment analysis engine is run across the contents including the learners' comments (suggestions/feedback). The comments are categorized as positive, neutral, or negative by the sentiment analysis engine. The learning materials are categorized according to subjectivity using the sentiment analysis results.

Again, a topic-level sentiment analysis model based on deep learning was introduced by (Pathak et al., 2021). This model uses a long short-term memory network's topic-level attention mechanism for sentiment analysis after extracting the topic at the utilizing online latent semantic indexing at the sentence level with regularization constraint. They also established the Gaussian Naïve Bayes classifier as the foundation model for the sentiment analysis. The accuracy of the model was reported to be 0.542. The authors (Sethi et al., 2020) created an algorithm that can accurately forecast the attitude that users will express on social media during the coronavirus outbreak. Unique classification methodologies were employed, while Support Vector Machines (SVM) and Decision Trees (DT) both performed incredibly well, the SVM classifier was more reliable and consistent throughout the study. Additionally, in research conducted by (M. Singh et al., 2021) respondents' feedback—that is comments or suggestions—expressed how they felt about the way the classes were done online. To evaluate the stakeholders' actions and reactions, opinion mining was also conducted on the quantitative responses provided by the respondents. The quantitative data is categorized using the sentiment analyzer feedback into three groups: positive, negative, and neutral, based on the feelings that are recovered. They came to the conclusion that higher education faculty members seem to be much more satisfied with the tools and methods of online learning than students are.

2.6 Privacy Preservation

(Buccafurri et al., 2016) proposes a protocol to protect user privacy while enabling analysis of social network likes. Based on cryptographic methods, this expands on the idea of likes by enabling users to link verified attribute values to likes. The goal of this protocol was to protect users' privacy while maintaining the ability to analyze likes associated with different aspects of persons. (Ivanova et al., 2022) explores the application and necessity of privacy-preserving algorithms in eLearning environments, with an emphasis on k-anonymity and (ε,δ)-differential privacy, to safeguard students' data and identities. In their experiment, they employed (ε,δ)-differential privacy and k-anonymity, evaluating the quality of data models, risk assessments, and machine learning-based prediction models to aid in decision-making. Moreover, (Aïmeur et al., 2007) emphasizes the need for privacy within eLearning systems and introduces an overview of Blind Digital Certificates, which do not expose the learner's identity. This framework was implemented and validated in an E-testing system scenario. (Yong, 2007) presents a systematic approach to designing digital identities for eLearning users, emphasizing the use of aliases to protect user privacy and preserve digital identities in an eLearning environment. They used XML meta-formats and alias transformation functions. In as much as these may be efficient privacy mitigation processing, privacy preservation should be a holistic approach where all the stakeholders in the eLearning domain has to play their part to ensure effective privacy protection. As (Ivanova et al., 2022) puts it “emphasis should be made on the need for a balanced approach to protect student privacy”. Similarly, (Nasukawa & Yi, 2003) also asserts

that a holistic approach is needed to mitigate the problem. So gleaning into the system and mining the opinions of the stakeholders in our case the student will provide a broader perspective of the security flaws that may manifest within the eLearning system.

Recent research has explored various approaches to address privacy concerns in text classification and representation learning. BERT-based models have been utilized for privacy requirements classification in issue reports, with N-gram IDF performing best among several techniques (Sangaroonsilp et al., 2023) To protect user privacy, a framework labelled DP_BERT was proposed, that learns differentially private text representations while maintaining utility (Alnasser et al., 2021). Another study introduced a homomorphic encryption method for BERT embeddings to prevent information leakage during text classification (G. Lee et al., 2022). In the context of privacy policy analysis, an XLNet-based model demonstrated improved performance over BERT in multi-label classification, achieving higher F1 scores without domain-specific fine-tuning (Mustapha et al., 2020). These studies collectively highlight the growing importance of privacy-preserving techniques in natural language processing and the potential of transformer-based architectures in addressing privacy challenges. However, in the literature, the synergy of sentiment analysis and privacy text classifiers has not been explored.

2.7 Nlp and sentiment analysis case studies in higher educational institutions elearning systems.

In the process of creating high-quality educational programs and courses, student input and opinions are now an essential part of quality assurance and control. “the provision of quality feedback is widely perceived as a key benchmark of effective teaching"(Alkhodair, 2023) More significantly, it makes instructors and institutions more receptive to students' needs and allows them to adjust when necessary. As a result, students in these kinds of schools feel encouraged, more involved, and partly in charge of directing their educational experience and surroundings to suit their tastes. Several case studies exemplify the successful integration of Natural Language Processing (NLP) and sentiment analysis techniques within eLearning systems in higher educational institutions, providing valuable insights into their practical application and impact. According to the literature, sentiment analysis has been utilized in educational settings to assist teachers in becoming more effective teachers and students in becoming better learners. (Baragash et al., 2022). For example, research was conducted to find out how the general population sees online education in light of post-reading habits on Twitter (Persada et al., 2020). The findings show a positive attitude in the direction of online education and provide information about the e-learning systems that students prefer. Moreover, (Balahadia et al., 2016) employed the machine learning algorithm Naïve Bayes (NB) and sentiment analysis tools to determine the teaching staff's strengths and weaknesses based on negative and positive student feedback. Similarly, (Newman & Joyner, 2018) analyzed student assessments of instruction

on a course utilizing VADER (Valence Aware Dictionary and Sentiment Reasoner), a sentiment analysis tool. They were able to identify frequently used phrases in the comments and compared positive and negative valences. The findings illustrated the usefulness of sentiment analysis as a technique for examining student evaluations of training as it provides a succinct synopsis of both the positive and negative elements of a given course. Moreover, according to (Baragash et al., 2022) By examining sentiment and satisfaction indicators in student posts, comments, and feedback, sentiment analysis has the potential to significantly enhance the teaching and learning process in higher education by assisting administrators and instructors in identifying students' trouble spots and taking prompt corrective action. Due to its effective application in social media analysis, sentiment analysis has gained recognition as a component of the text mining research field (Laksana et al., 2018). In a study (Mujahid et al., 2021) they employed social media data to analyze stakeholder sentiment, and they looked at the efficacy of online education. A lexicon-based technique was utilized to discover the label tweets and sentiments. Bag of Words (BoW) and Term Frequency-Inverse Document Frequency (TD-IDF) were used to classify positive, negative, and neutral sentiments utilizing feature engineering techniques and a number of machine learning techniques. By using data balancing with the Synthetic Minority Over-sampling Technique (SMOTE), they reported 95% classification accuracy for Random Forest (RF), Support Vector Machine (SVM), and Decision Tree (DT) classification algorithms.

2.8 Emerging trends and future directions

Regarding Natural Language Processing (NLP), emerging trends are reshaping the landscape of privacy-preserving technology integration, particularly within the domain of e-learning systems in higher educational institutions. Recent studies by (Jim et al., 2024) and (Gunasekaran, 2023) have highlighted the growing importance of sentiment analysis techniques in safeguarding user privacy while enhancing the educational experience. These advancements underscore a paradigm shift towards more nuanced approaches to data handling and analysis, where the sentiment of users' interactions with e-learning platforms is leveraged to personalize experiences without compromising privacy (Jim et al., 2024) Moreover, the integration of machine learning algorithms, such as deep learning models, has demonstrated encouraging outcomes in automatically identifying and redacting sensitive information from textual data, ensuring compliance with privacy regulations like GDPR and HIPAA (Gunasekaran, 2023)

Looking ahead, future directions in NLP-based privacy preservation hold immense potential for revolutionizing e-learning systems in higher education. As articulated by (Le et al., 2024) one promising avenue is the exploration of federated learning frameworks, wherein machine learning models are trained collaboratively across distributed devices while keeping user data localized and encrypted. This approach not only mitigates privacy concerns by minimizing data exposure but also enables the creation of stronger and contextually aware NLP models tailored to the particular requirements of every student (Le et al., 2024). Additionally, the fusion of NLP with emerging technologies such as blockchain offers novel solutions for

transparent and auditable data management, ensuring trust and accountability in educational settings (Idrees & Nowostawski, 2024). By embracing these emerging trends and future directions, researchers can propel the field of NLP-based privacy-preserving technology integration forward, paving the way for more secure, personalized, and effective e-learning experiences in higher educational institutions. From the literature reviewed evidently, sentiment analysis has been used extensively across several fields, but its use in the context of eLearning privacy remains relatively unexplored. Particularly regarding the lack of sentiment analysis specifically focused on students' feedback regarding privacy and security issues in eLearning platforms. Moreover, a privacy classifier to identify prevalent privacy issues on the eLearning platforms has been understudied. Hence, this study aims to divulge the perceptions and sentiments of students on their privacy in eLearning systems to explore the privacy issues that the learners face. We aim to lay the groundwork for proposing a methodology to leverage sentiment analysis and a privacy classifier to establish a holistic privacy preservation approach in higher educational institutions' eLearning platforms.

In summary, sentiment analysis has proven to be effective in modelling course structure, enhancing user experience and personalization of delivery content on various eLearning systems; commercial and non-commercial. Moreover, it has been used to evaluate the acceptance and adoption of eLearning systems. Despite its widespread usage in various domains such as e-commerce, its practicality in eLearning systems '—' specifically privacy preservation and security has not yet been explored. Therefore, moving forward to the next chapters, we will build upon

the gap identified in the literature review, and propose and develop a methodology aimed at subtly addressing privacy concerns in eLearning platforms.

CHAPTER THREE

3.1 Introduction

Several privacy issues, including identity theft and discrimination, can arise from improperly using personally identifiable information collected online (Humphreys et al., 2010). Maintaining privacy is crucial for consumers of contemporary information systems (Azemović, 2012). Although the architecture and content for the eLearning system have been developed with a great deal of work, the system's security has received very little attention (R. Ali & Zafar, 2017; Bhatia & Maitra, 2018; Kritzinger, 2006). In this chapter, we discuss the approach we adopted to get learners' privacy insights/opinions. We aim to develop effective sentiment analysis and privacy classifier models that can be incorporated into eLearning systems. Specifically, we will leverage the predictions from a sentiment analysis model to selectively apply the privacy classifier model. As sentiment analysis determines the polarity of a piece of text, the privacy classifier, on the other hand, is tasked with identifying the prevalent privacy issues in the eLearning system from the textual data. This chapter introduces the methodology for building the sentiment analysis and privacy classifier model.

As observed in the literature, substantial research has been conducted on sentiment analysis and text classification. However, the synergy of both scenarios is yet to be explored. In effect, the methodology proposed combines sentiment analysis and text classification models to provide a holistic approach to privacy

preservation on the eLearning systems. We used the existing deep learning architectures and algorithms already explored in many different fields, such as pattern recognition, computer vision, and natural language processing (Onan, 2021). Moreover, as (Estrada et al., 2020) observed in their study that Deep Learning models especially in learning situations, BERT outperformed conventional machine learning techniques in the classification of opinions. That said, we leveraged transfer learning to complement our insufficient dataset and fine-tuned the BERT-Pretrained model to train both models. The suggested transfer-learning approach has the benefit of using transferred domain knowledge, acquired through a neural network trained on a sizable auxiliary corpus. This knowledge can be applied to produce predictions for any unlabeled or labelled real-time testing data. In the subsequent subsections, the techniques that were used to build the models are discussed

3.2 Models Techniques

3.2.1 Word representations and word embeddings

For machine learning models to process words, they must have a numerical representation allowing them to do computations. These words are represented as low-dimensional, dense vectors called word embeddings in a continuous vector space (Ding, 2019). Word embeddings are better choices for learning syntactic and semantic knowledge (Khan et al., 2022). As traditional word embeddings are usually sub-optimal besides, it slows down the training processing of the model (Y.

Li et al., 2017). In this, words with similar meanings or contexts are clustered more tightly. There are several word embeddings: Pennington and associates published Global Vectors for Word Representation (GloVe) in 2014 (Pennington et al., 2014) Word2Vec, WordPiece are all standard word embedding components of most state-of-the-art NLP architectures including the transformer and many others (Mikolov et al., 2013; Pennington et al., 2014). Given this, we used the Glove word embeddings to represent our text data during the model training.

3.2.2 Transformers as *Feature Extractors*

Transformer is a stack of encoders and decoders. Which uses attention to boost the speed with which models can be trained. In the transformer, self-attention computes a representation of a single sequence by relating its many places (Vaswani et al., 2017). The model uses self-attention to interpret the information it is given. A series of words can be processed simultaneously by the Transformer model. As a feature extractor for our classifier models, we utilize a transformer. We keep the transformer's weights frozen during training and use the concealed states as the classifier's features. This approach allows us to efficiently train a streamlined model, such as a neural classification layer that doesn't rely on gradients. This idea was used by (Tunstall et al., 2022) in their study. By leveraging the robust feature extraction capabilities of the transformer, we hope to achieve high performance with a more efficient and focused model.

3.3 Data Description

Making decisions, whether at the individual or the organizational level, is invariably paired with seeking out the opinions of others (P. K. Singh & Husain, 2014). Every Natural Language A piece of text, such as customer reviews regarding a particular online order, is the starting point for a natural language processing (NLP) activity.(Tunstall et al., 2022). (Estrada et al., 2020) noted in their research that the quality of the expression datasets has a significant impact on the classifiers' output. For this study, an online questionnaire was floated in the three Higher Institutions to enhance the data collection. Two objectives guided the survey's design: to comprehend the students' opinions/sentiments of student textual data on whether a learning process infringes on their privacy or the eLearning platform and also to build a privacy classifier model that will help predict the most prevalent privacy issues on the eLearning platform. According to (Prasad & Nakka, 2023), student feedback is essential for the highest standards and quality of education. During the data collection phase, the participants were mainly asked about their educational backgrounds, their higher institution names, and generic questions about their sentiment or perception of the privacy of the eLearning system, and more about what issues they might have faced while using the e-learning platform. Moreover, some predefined privacy issues were listed and the participants were requested to provide more detailed descriptions of any of those issues they might have experienced. This description will help build the privacy classifier model. Building a deep learning model with a huge amount of data, we had a few sample responses from the students that might not suffice for the training of the models so

various techniques such as web scrapping were used to scrap privacy-related text from the internet (Reddit and Wikipedia) and we manually annotated them to reflect the specific privacy issues in the questionnaire and the sentiment of those data were equally annotated as either positive or negative. Moreover, some text corpus from Kaggle was also gleaned and appropriate text was selected and included in the dataset for the training of the model. Specifically, the cyber threat dataset from Kaggle was used to train the privacy classifier. This dataset offers an extensive compilation of data for detecting, diagnosing, and mitigating cyber threats using textual content, and entity relationships.

3.3.1 Data Preprocessing and Augmentation

In the Kaggle data set not all the columns we so relevant in this regard hence those were eliminated. Moreover, some of the records were merged as they have similarities. The columns that were merged include the malware and identity; these were added to the already defined privacy class, identity theft. Again, the location column in the cyber threats data was merged with the already defined privacy class; location tracking the justification was that location incident could be present with this text and the privacy model could be able to identify some element of location tracking within the data. In NLP tasks, especially those involving classification problems, id2label, and label2id dictionaries are used to map class labels (categories) to integer IDs and vice versa. These mappings are essential for various stages of the NLP pipeline, such as data preprocessing, model training, and evaluation. To feed text data into an NLP model, the text must first be tokenized and then converted into numerical values. Similarly, class labels must also be

transformed into numerical representations. The label2id dictionary helped in converting the original class labels into integer IDs. NLP models usually output probability distributions over classes as their predictions. During training, the model's predictions are compared against the ground truth labels (which have been converted to integer IDs) to compute the loss and optimize the model parameters.

As noted earlier, the fewer responses we have translated that we augment the dataset at our disposal to obtain substantial numbers for the training of the models. Using techniques for augmenting data to create additional training samples from the current ones is a straightforward yet efficient method of improving text classifier performance on limited datasets. (Tunstall et al., 2022). This became very imperative due to the small training dataset we had. In practice these were the two ways of data augmentation techniques we employed:

Back translation

We used machine translation to convert the material from English, the source language, into one or more target languages, such as German and French, and then back to English. High-resource languages or corpora with few domain-specific terms are typically the best candidates for back translation (Sennrich et al., 2015; J. Xu et al., 2023; D. Zhang et al., 2023)

Token perturbations

Additionally, we randomly select and carry out basic transformations, such as random synonym replacement, word insertion, swap, or deletion, using the training set's text. According to earlier studies, training language models on tokens rather than sentences directly produces more reliable classification results (Kamp

et al., 2022). Combining these two data augmentation techniques we hope to obtain good classification accuracy from the models.

3.4 Models' Development

The proposed methodology is in two steps: a) Using the BERT pre-trained model to develop the sentiment analysis model. b) And also developing a privacy classifier model that will be invoked when the former model's output polarity is negative.

3.4.1 The Sentiment Analysis Model

Due to its capacity to efficiently capture contextual information in sequential data, the Transformers Bidirectional Encoder (BERT) pre-trained model was utilized to take advantage of the limited dataset available to us. We also adopted the BERT model to leverage its attention mechanism to capture relevant features and semantic relationships within the textual data. We then fine-tuned this model passing our custom data to it and adjusting various hyperparameters, after applying rigorous data preprocessing techniques specified earlier. Below is a high-level overview of the sentiment model.

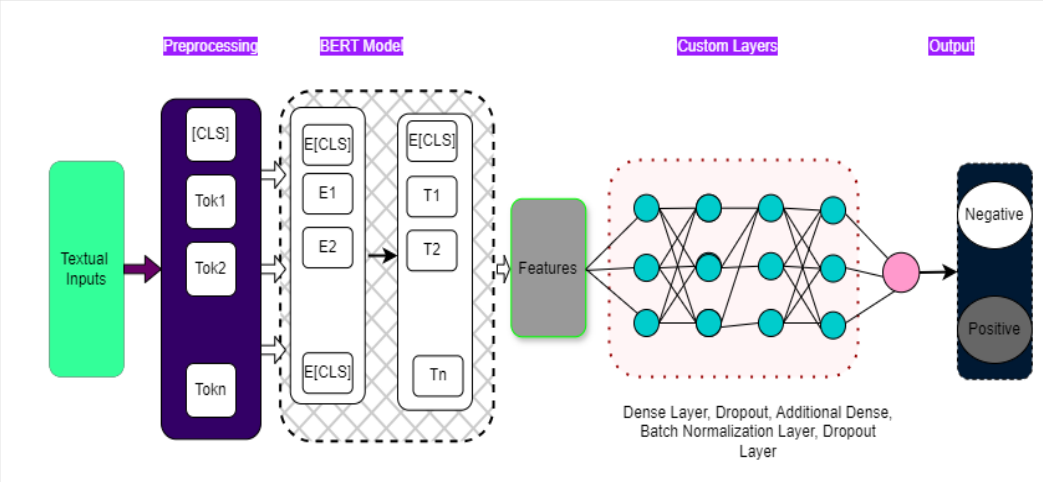

Figure 1The Sentiment Analysis Model

Custom Neural Network (NN) layers were added to further learn and extract relevant features from the BERT output features. A batch normalization layer was added in the same procedure to prevent internal covariate shifts, which can impede training and make selecting appropriate hyperparameters challenging. To solve this problem, batch normalization normalizes each layer's activations in a mini-batch of data (Ergen et al., 2021). Moreover, a dropout layer is added to “choke” out some nodes, so its information is not propagated to the next layer. This helps to prevent overfitting; since Neural Networks (NN) tend to have many layers, with a great multitude of parameters, and can thus be trained to match the training data quite exactly. Ultimately, the class probabilities are propagated as outputs using the sigmoid activation function.

3.4.2 The Privacy Classifier Model

Following the sentiment analysis model, we proceeded with the development of the privacy issue classification model. Leveraging techniques such as word embeddings, we designed a model to identify specific privacy concerns within textual data, including location tracking, identity theft, and data leakage. The same BERT was also used in this case due to the advantages specified above over other machine learning models. The embedded input sequence is then processed through the BERT model's encoder layers, which consist of Feed-forward neural networks and self-attention processes. In the process, the model gains the ability to recognize any links between the tokens as well as the syntactic and semantic information contained in the input sequence. At the end of the BERT model's encoder layers, each token has a corresponding hidden state vector. For the [CLS] token, its final hidden state is used as an aggregated representation of the entire input sequence. This vector is then passed to the task-specific classification layer. The final hidden state of the [CLS] token is fed into a linear layer, which maps to a vector of size equal to the number of target classes. This is essentially a weight matrix multiplication followed by a bias term addition.

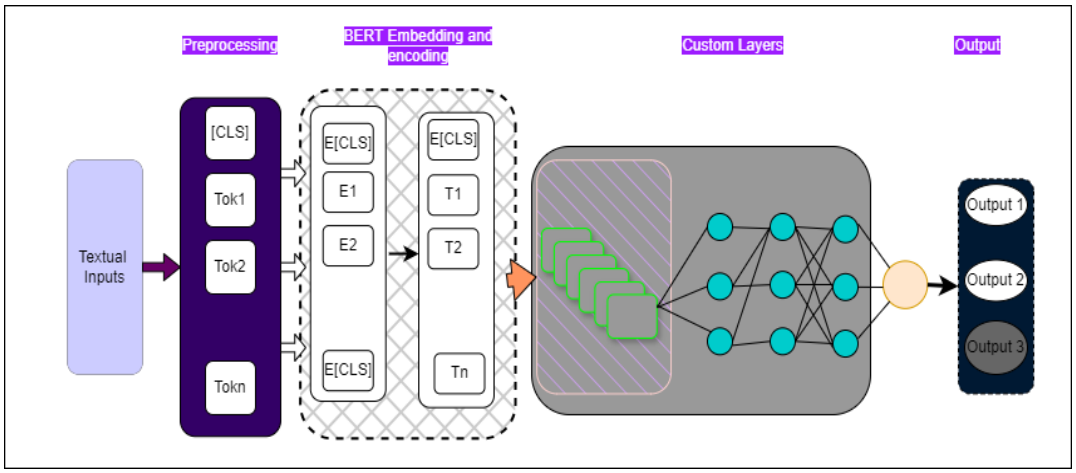

Figure 2The Privacy Classifier Model

As previously said, after merging those feature vectors, the model receives lexical (word token) features as input and syntactical features—technically known as "dependency parse tree information"—as input. Before undergoing an extra multi-layer perceptron stage, these vectors are later combined with other (auxiliary) inputs. The probability for each of the aforementioned privacy classes is provided by a single neuron or SoftMax function at the end of the deep neural network.

3.4.3 Models Inputs and Outputs

A series of words that continue to travel up the stack are fed into BERT (S. Wang et al., 2020). After applying self-attention, each layer transfers its output to the subsequent encoder via a feed-forward network. Each of the encoders in the model extracts relevant information from the input text and then forwards it to the next encoder. A vector of size *hidden* size is output for every place, word, or element. We just pay attention to the output of the first slot (where we passed the special [CLS] token) for our models. That vector is now used as the output for our models. Since our targets are more than one, we tweaked the classifier network to

have more output neurons. A SoftMax function is then applied to the linear layer's output, transforming the raw output values into class probabilities. The total of probabilities is guaranteed by the SoftMax function across all the 3 classes equals 1.

3.4.4 Layered Approach to the Sentiment and Privacy Models

The cascade/ hierarchical approach is an interesting technique that was used to combine both the sentiment analysis and privacy classifier models. In the cascade/hierarchical approach, we trained the primary model; the sentiment analysis model to make the initial prediction. Based on the output of this primary model, we selectively apply the secondary model; the privacy classifier model. In general, if the sentiment prediction is positive, no further processing is required, as we assume that positive sentiment is unlikely to raise privacy concerns. Contrary if the sentiment prediction is negative, we now invoke the privacy classifier as negative sentiment could raise a privacy concern.

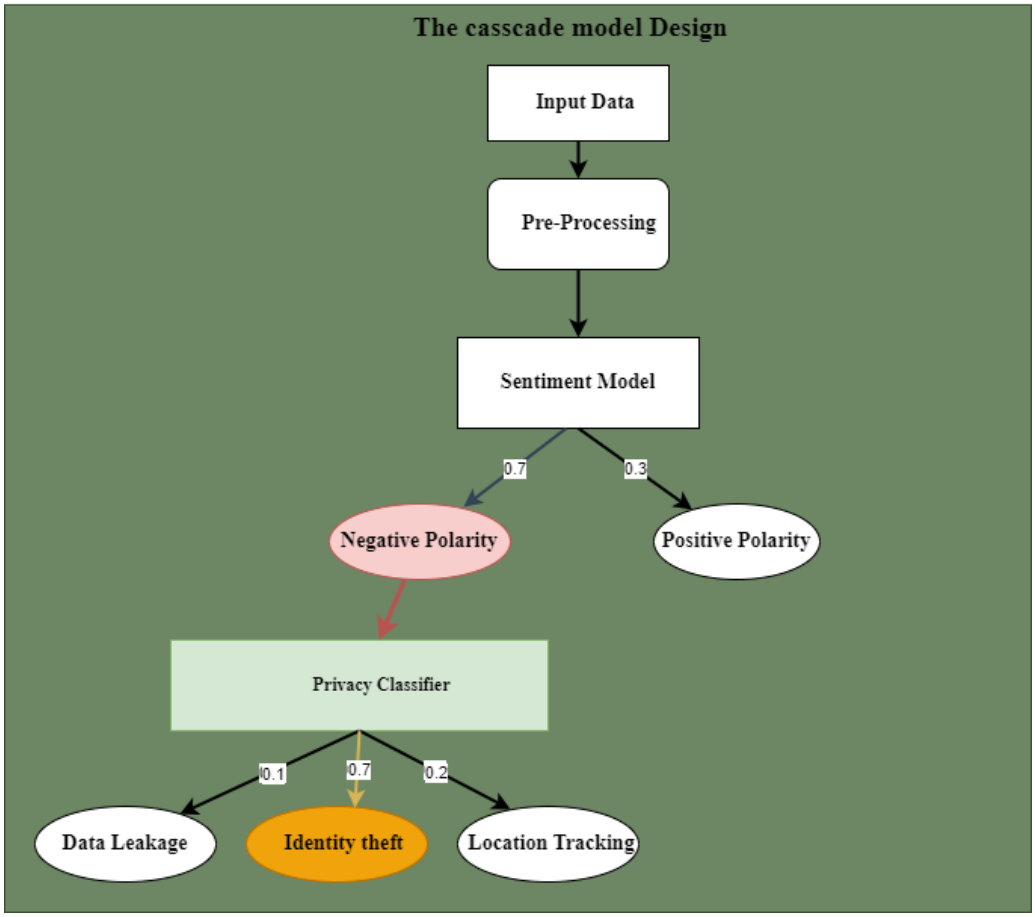

Figure 3The Casscaded Model Design

The primary motivation behind this approach is to leverage the strengths of each model in a hierarchical manner, where the secondary model is only invoked, when necessary, based on the primary model's output. This can potentially lead to computational efficiency by avoiding unnecessary processing by the secondary model in certain cases.

Key advantages of the cascade/hierarchical approach:

1) **Computational Efficiency**: By selectively applying the privacy classifier model only when the sentiment is negative, potentially saves computational

resources and time, especially since the privacy classification task is computationally expensive due to the layers in the model's architecture.

2) **Modular Design**: This approach allows for a modular design where the sentiment analysis and privacy classification components are developed, trained, and optimized independently.

3) **Flexibility**: This method is flexible and can be extended to include additional models or processing steps, depending on the difficulty of the task or the specific application requirements.

4) A key component of assessing the effectiveness of Natural Language Processing (NLP) models is empirical evaluation (Goutte & Gaussier, 2005). This corresponds to the final evaluation that the model goes through after the training phase has been completed. At this stage to analyze the performance of the model, we use precision, accuracy, F1-score, and recall which are predominantly used (Fourure et al., 2021). This step is critical to test the generalizability of the model by using a test set we can accurately estimate the effectiveness of the model on unseen data. Once the model has been trained, its predictions (in the form of integer IDs) need to be mapped back to their original class labels to make the results interpretable. The id2label dictionary is used to perform this conversion.

In summary, the experiment performed in this research followed a series of steps as described: Collecting the data through a questionnaire and from various online platforms including Wikipedia, Reddit, and Kaggle. The questionnaire was

distributed to e-learning participants who are students in the selected Higher Institutions. Data preprocessing includes the manual annotations of some of the datasets into the positive and negative and the targeted privacy issues in the corpus. The transformer architecture was used due to its structures to capture dependencies between the inputs, subsequently, we leverage transfer learning and the Bidirectional Encoder from the Transformer (BERT) pre-trained model.

CHAPTER FOUR

4.1 Introduction

In this chapter, the results and discussion on performance measures, experimental procedures, and results obtained after building the model, as well as the research questions and objectives set out at the beginning of this study. The main objective of this research was to explore privacy concerns within higher educational institutions' eLearning platforms and develop a Natural Language Processing (NLP)-based model using sentiment analysis to identify the most prevalent privacy issues — thus providing knowledge-based for privacy preservation decision-making. Also, we provide a comprehensive discussion on how sentiment analysis can be employed to detect privacy concerns, the specific privacy issues identified through negative sentiments, and the potential of integrating sentiment analysis and privacy classification models into eLearning platforms to manage and mitigate privacy risks and enhance privacy preservation.

Our suggested methodology can be summed consisting of a hierarchical model in which the execution of the second model is dependent on the first model. Thus, the sentiment model runs, and if the predicted sentiment polarity is negative then the second model: the privacy classifier is invoked. Nonetheless, if the sentiment polarity is positive the second model is never invoked.

In effect, our subtle goal is building knowledge bases through sentiment analysis and a privacy classification system. Specifically, we use a combination of deep

learning models trained across general knowledge areas and natural language processing approaches. In this way, we developed two models which were finally cascaded. In the end, the sentiment and privacy issues are collected over time providing a rich knowledge base for effective security and privacy evaluation on the learning system. This study, however, intends to offer support to learning management for their privacy-preserving tasks.

4.2 Models Performance Measures

We harnessed the capabilities of the BERT pre-trained model to fine-tune both our sentiment analysis model and the privacy classifier. This section evaluates the effectiveness of the two key models developed in this study: the sentiment analysis model and the privacy classifier model. Each model's effectiveness is measured against specific metrics to determine its reliability and accuracy in addressing the research questions and objectives. The evaluation is based on several key metrics that assess the model's precision, accuracy, recall, and overall performance in predicting sentiment and identifying potential privacy issues in user responses. Responses from users that include at least one aspect of a privacy problem are considered privacy-related. Responses that don't include any mention of privacy are considered non-privacy-related.

Parameters Setting and Performance Evaluation Metrics

There are several parameters to tune. In this research, several experiments were conducted to find the optimal parameters. Only the parameters that yielded the best results are reported. For this study, we set the training size to be 80% of the whole dataset, and the remaining 20% for testing. We set the number of epochs to

10 for all the experiments. The dropout rate is set at 0.5 to regularize the neural networks and prevent over-fitting issues. Next, we used the test datasets and common metrics to validate the model's performance. This study has taken into account classification accuracy, F1-score, and precision to assess the effectiveness of machine learning models. According to (Khan et al., 2022; Onan, 2021), one of the most used metrics for assessing supervised learning models, such as sentiment analysis and text classification, is classification accuracy.

Which is calculated by Equation (1).

$$\text{ACC} = \frac{TN+TP}{TP+FP+TN} \quad \textbf{Equation (1)}$$

The numbers of true negatives, true positives, false positives, and false negatives are indicated by the letters TN, TP, FP, and FN, respectively.

Where TP is the number of sentences that are positive and predicted correctly as positive, FP is the number of sentences that are negative and predicted incorrectly as positive, TN is the number of sentences that are negative and predicted correctly as negative, and FN is the number of sentences that are positive and predicted incorrectly as negative.

As shown in equation (2), precision is another widely used metric that calculates the ratio of true positives to both true positives and false positives.

$$\textbf{Precision} = \frac{TP}{TP+FP} \quad \textbf{Equation (2)}$$

Additionally, according to equation (3), recall is the ratio of true positives to both true positives and false negatives.

Recall = $\frac{TP}{TP+FN}$ **Equation (3)**

Based on Equation (2) and Equation (3) the F-Measure is calculated as

F-measure = $\frac{2*Presision*Recall}{Precision+Recall}$

4.3 Overview of the key finding

Several issues prevailing on the internet were identified through an in-depth literature review.

The security issues identified on the internet are:

- Malware
- Cybersecurity attacks
- Data storing vulnerabilities
- Potential data leaks due to lack of user experience, or system misconfiguration.

These security issues can affect user privacy and security on the eLearning in the following ways:

- Data leaks and breaches can eventually expose users' personal information
- Lack of user awareness and understanding of eLearning systems security and privacy risks
- Vulnerabilities in how user data is stored and managed by the eLearning management and also
- Challenges in identity management and controlling access to user data

Since eLearning thrives on internet protocols, it is quite safe to equate a significant amount of privacy issues related to the internet to eLearning platforms.

These protocols are significant for content delivery, communication, and data exchange, which inherently exposes the learning systems to similar privacy risks as other internet-based services.

According to the data collected from the study site, most of the responses from the students suggest a positive sentiment toward eLearning. However, their responses are mainly towards eLearning effectiveness, its adoption and helpfulness and not necessarily their privacy. This could result from massive literature, study, or research towards the effective evaluation, acceptance, and implementation of eLearning without much consideration of privacy and security on the eLearning systems. As noted by (Aïmeur et al., 2007; Bhatia & Maitra, 2018; Kritzinger, 2006) research. Nonetheless, a few responses from the survey suggest privacy concerns on the learning platform. The augment was that the learning platforms are mostly web applications that leverage internet protocols as stated earlier and therefore privacy should be a concern. (Roussos et al., 2023) elaborate some consequences of failing to provide a degree of reliability and security in an effective eLearning system. The graph below shows the privacy issues that were used as a target for our privacy classifier model. Considering the dataset used for the model development a brief overview is displayed below. Figure 1 shows the distribution of the privacy issues identified for the classifier and Figure 2 shows the distribution of the sentiment. Note that not all the data were collected from the students' others we mined from online repositories identified in Chapter 3.

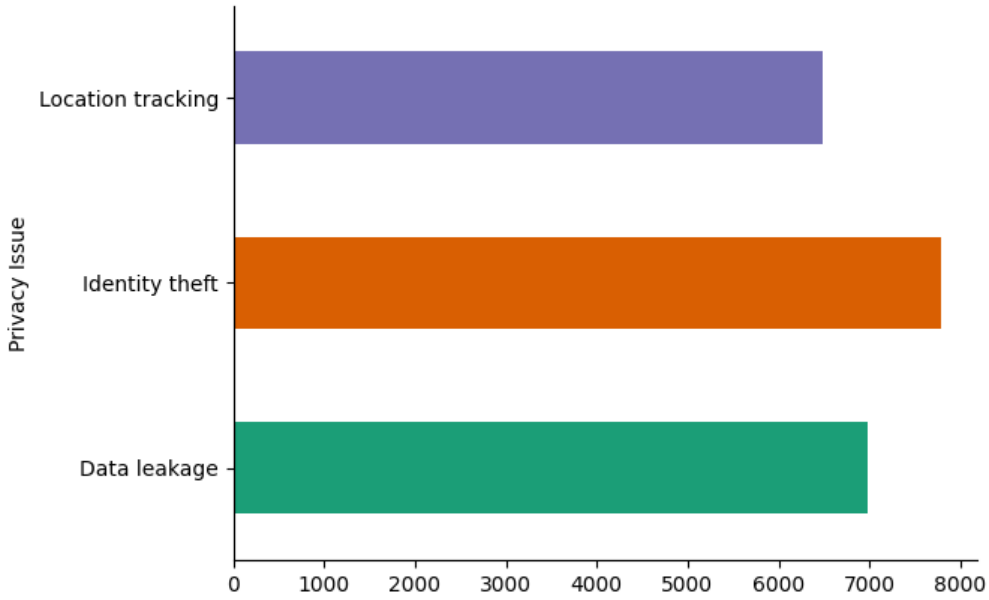

Figure 4: Shows the Privacy Issues Counts

The graph below also shows the count of the sentiment labels in our dataset.

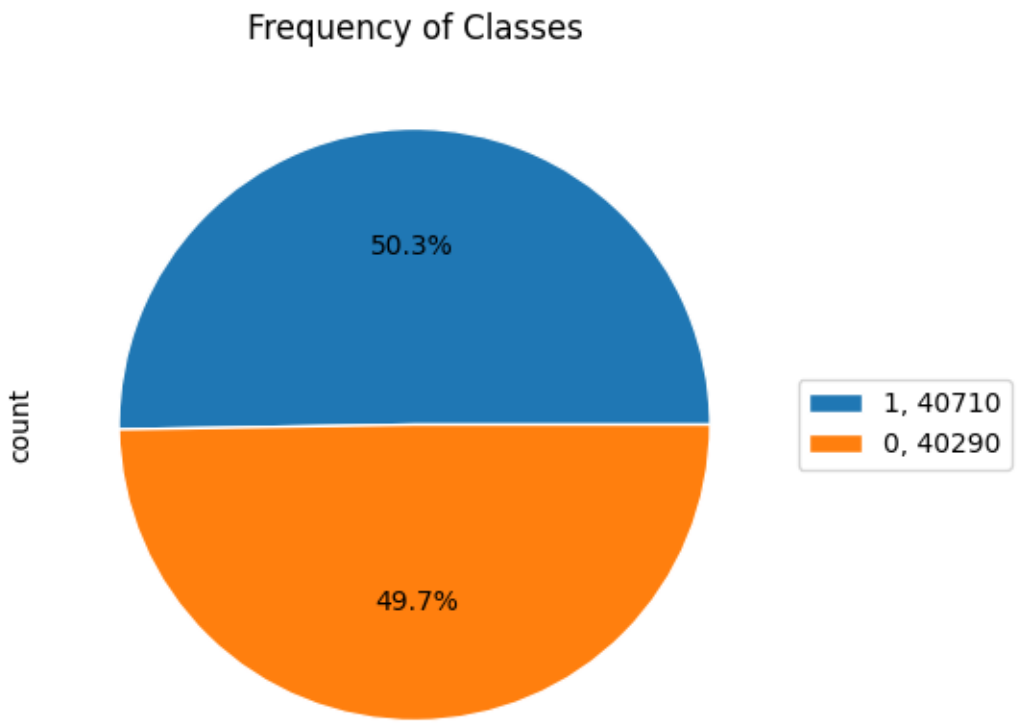

Figure 5: Shows the Both sentiment Polarity Counts

4.3.1 Sentiment Analysis Model

This analysis will help provide a better understanding of the model's performance and its ability to capture the sentiments from the responses. To put it simply, a deeper comprehension of users' views on privacy in the e-learning system can be obtained in order to improve it. These metrics obtained indicate that the model performs well in classifying user sentiments as positive, or negative. The figure below shows the metrics and their values. However, it is worth noting that

some limitations were observed, particularly ambiguity in student feedback which led to occasional misclassifications.

	Metric	Training Set	Validation Set
0	loss	0.023581	0.001171
1	accuracy	0.993908	0.999753
2	precision	0.993908	0.999753
3	recall	1.000000	1.000000

Figure 6 Evaluation metrics for the sentiment model

The F1 measure is a weighted average of Precision and recall, and for accuracy, it simply reports the ratio of correctly classified sentences regardless of their class. In other words, the higher the Precision, the more accurate the prediction of the positive class. The high recall indicates a high number of sentences from the same class are labelled to their exact class. We also used the ROC to further evaluate the sentiment classifier performance comprehensively. A graphical representation of a binary classification model's performance is called a ROC curve.

Below is the ROC curve for the sentiment classification model.

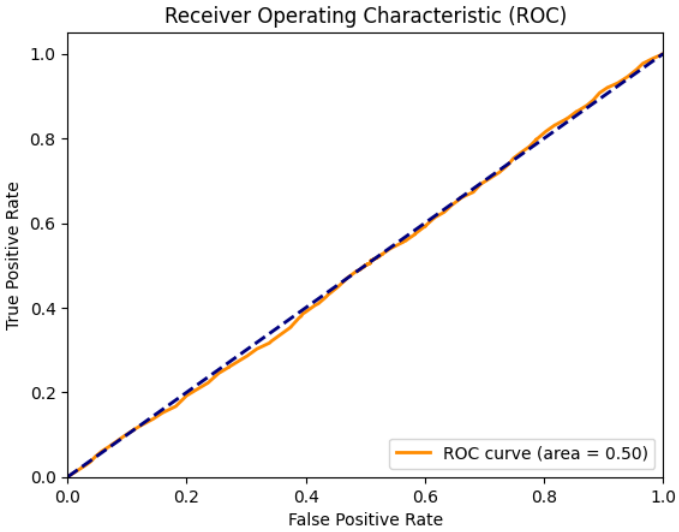

Figure 7 ROC curve for the sentiment model

Confusion Matrix

The confusion matrix was used to assess the validity of the sentiment model. The diagram below shows the model's confusion matrix.

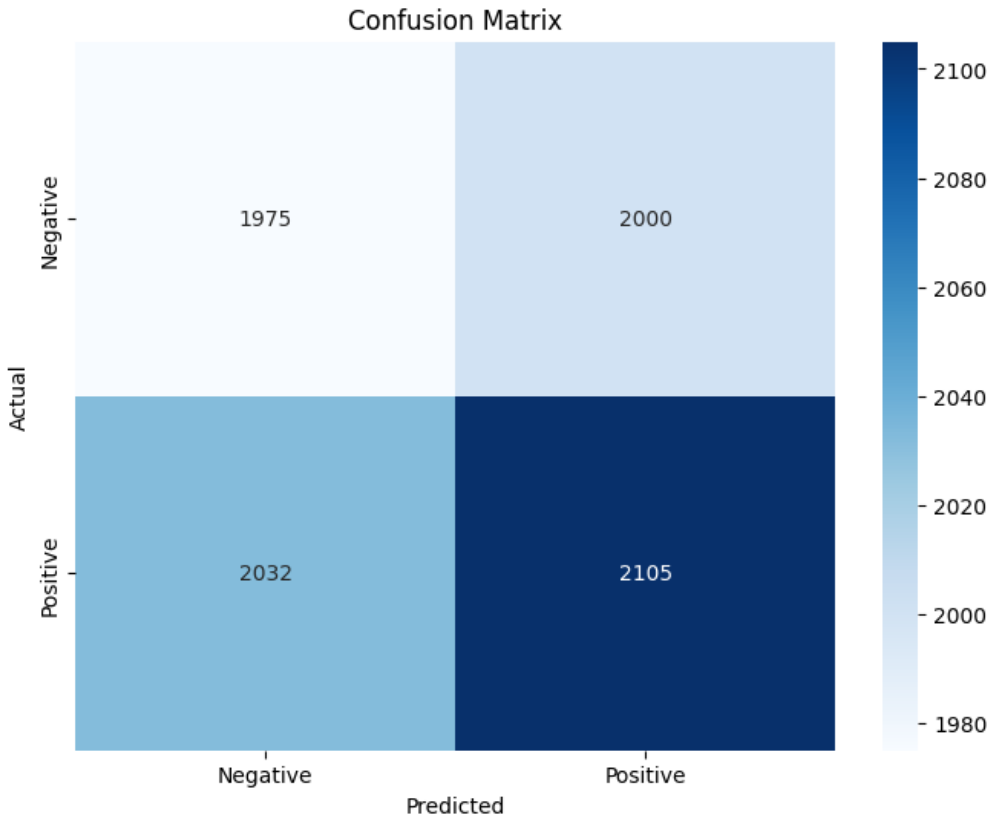

Figure 8 The Sentiment Model confusion matrix

From the graph above the following inferences can be made.

1. True Negative
    - These are the instances where the actual sentiment is Negative and the model correctly predicted it as Negative.
    - There are 1975 instances in this category.
2. False Positive
    - These are the instances where the actual sentiment is Negative, but the model incorrectly predicted it as Positive.
    - There are 2000 instances in this category.
3. False Negative

- These are the instances where the actual sentiment is Positive, but the model incorrectly predicted it as Negative.
- There are 2032 instances in this category.

4. True Positive
    - These are the instances where the actual sentiment is **Positive** and the model correctly predicted it as **Positive**.
    - There are 2105 instances in this category.

Ideally, the model's performance is almost equal for both classes in terms of correct predictions (1942 negatives, 2080 positives).

4.3.2 Privacy Classifier Model

Confusion Matrix

The confusion matrix was used to assess the validity of privacy classifier models. The diagrams below show the privacy classifier's confusion matrix. Only 24.40% of Identity theft were mislabeled as Location Tracking and 11.0% as Data Leakage, while 65.0% were classified accurately as Identity theft. Only 15.00% and 00.0% of Location Tracking were misclassified as Data Leakage and Identity theft, respectively, while 85.0% of Location tracking was classified accurately. Only 27.0% and 0.00% of Data leakage were misclassified as Location tracking and Identify theft, respectively, while 73.00% of Data leakage was classified accurately.

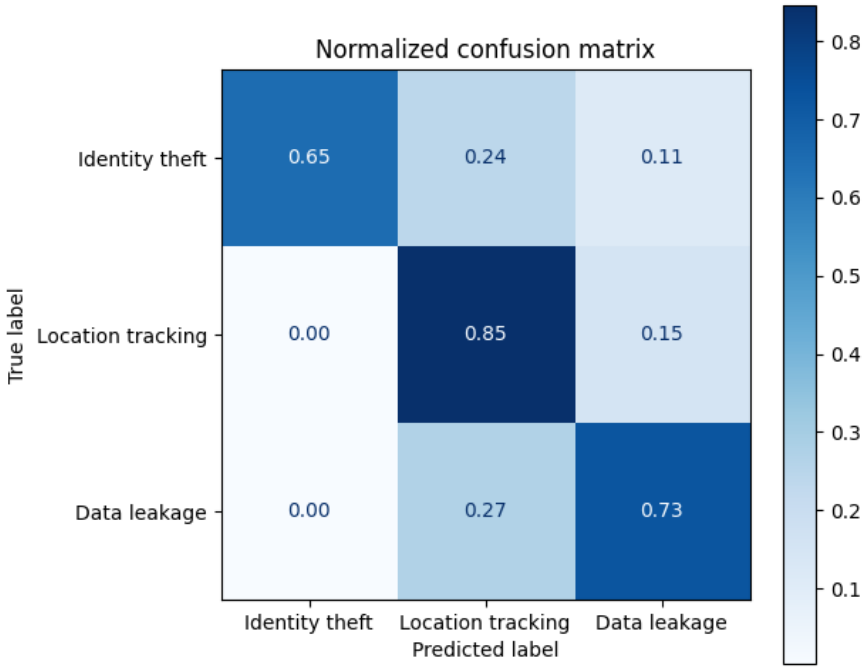

Figure 9: Confusion Matrix for the Privacy Classifier

Error Analysis

Another explicit metric that is being used to measure the generalization of a model is the loss of the classifier. Loss measures how well or poorly the model's prediction matches our data's actual or ground truth classes. In other words, it quantifies the predicted output of the model and the ground truth labels. The CrossEntropyLoss was used in this regard. The table below shows the loss obtained during the test for each of the test data. The first table shows a relatively large loss value for the test data. Subsequently, the loss was reduced to improve the generalization of the model's performances. The techniques used are indicated in the previous Chapter where we added regularization to avoid overfitting and

underfitting, added a couple of dropout layers, and set the rate to 0.5. performed data augmentation etc.

Before continuing, we took a closer look at the predictions made by our model. To arrange the test samples according to the model loss, we used a straightforward yet effective method. As soon as we cross the label during the forward pass, the loss is instantly determined and returned. The table below shows a sample of the test data actual label and the predicted loss metric for each of the sentences in the test dataset. In the two figures below, we combined the text, the actual label, the predicted label and the loss for each of the text during the training. Afterwards, the data was sorted based on the losses. Figure 4 was sorted based on the maximum loss value and Figure 5 was also sorted based on the smallest loss.

We could see that the smaller the loss the better or more accurate the model becomes and contrary, the model deviates from predicting the correct ground truth labels.

Sorted based on larger Loss

TEXT	ACTUAL LABEL	PREDICTED LABEL	LOSS
This is my girlfriends Instagram account. Due ...	Identity theft	Data leakage	7.424717
This is my girlfriends Instagram account. Due ...	Identity theft	Data leakage	7.424717
This is my girlfriends Instagram account. Due ...	Identity theft	Data leakage	7.424717
Part of the AT&T breach as I'm sure many o...	Identity theft	Data leakage	7.064817
Part of the AT&T breach as I'm sure many o...	Identity theft	Data leakage	7.064817
Part of the AT&T breach as I'm sure many o...	Identity theft	Data leakage	7.064817
hi all, dealing with an awful mess im trying t...	Identity theft	Location tracking	6.708397

Figure 10: Bigger Loss and Actual and Predicted Labels

Sorted based on small loss

TEXT	ACTUAL LABEL	PREDICTED LABEL	LOSS
boat. It needs to have a battery life of more than 1 month, be waterproof and no monthly plan. Is there a GPS tracker that only charges me if I use the tracking service? I'll only need to	Location tracking	Location tracking	0.000324
Has anyone found the salt in the long time?	Data leakage	Data leakage	0.176070
ny playlists there. i just recently got an email saying my email address was just changed to: rodajeproduccion2018@gmail.com. which is not my email address and now i am locked out of emailed customer support and they want i would consider some private information. and i didnt feel comfortable sharing that info through email. so i called their customer support number 1- super loud. he didnt even say spotify or a company name. i told him what was wrong and he wanted a 4-step verification method. my full name, phone number, DL#, my bank statement hat? they already hacked my account online why would i give more information to them. hes no its a security measure. so before i gave any more information i was like ok what next. hes oing to have to connect to your computer!?! (WHAT? i thought only apple does that when you need to fix something) and im like ok no thanks and HUNG UP! was i wrong? am i the only one back?	Data leakage	Data leakage	0.001599
The lender has run my credit and I was able to place my freeze back on Transunion and Experian. But Equifax will NOT let me place my freeze back. I did unfreeze my files until Jan 30, il Jan 30. That's NOT ok for me. Anything I can do to get the freeze back NOW? TIA.	Identity theft	Identity theft	0.003531
reach-in-london-ulez-fine-enforcement**](https://www.theswedishtimes.se/articles/belgium-investigates-data-breach-in-london-ulez-fine-enforcement)	Data leakage	Data leakage	0.044277
lass-action-settlement-notice-heres-what-to-consider-when-deciding-to-join-or-opt-out: It might have happened to you a few times in past years: You received an email or mail notice inviting omatically included. But being part of such a lawsuit might be intimidating, especially if you need to opt in, and would mean surrendering the option to sue individually. In most cases, there's ns — often thousands — into one claim against a single defendant, reducing fees for each claimant and potentially earning a much larger payout. And there have been many opportunities illion-dollar class-action settlements in U.S. history apart from the tobacco settlements decades ago, according to a report from the national law firm Duane Morris. The stakes are high for sponsibility in areas such as data privacy, employee discrimination, securities fraud and civil rights. Advertisement But in cases where you suffered significant harm, suing individually could	Data leakage	Data leakage	0.001546

Figure 11:: Smaller Loss and Actual and Predicted Labels

In the output layer as discussed, the class probability of the ground truth labels is obtained using the SoftMax function, and the class with the highest probability is presented alongside the predicted label. The graph below shows the class probabilities of the various classes and the predicted class having the highest probability value. The class probability against the actual labels shows the dominant class in the sample test data provided.

Testing with new data

We tested the model with sample test data to plot the class probabilities against the actual labels to show the dominant class in the sample test data. The class in the test data is Data leakage with the highest probability which is approximately 95%.

See the graph below.

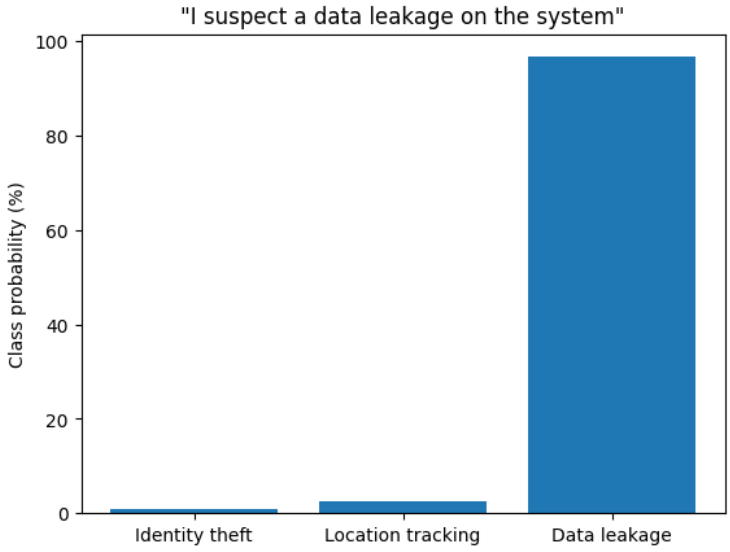

Figure 12: Sample text and label class probability Prediction

The aforementioned evaluation results serve as a basis for the discussion that follows regarding how well these models respond to the research questions and achieve the goals that were established at the outset of this investigation.

4.4 Discussion on research question 1

Research Question 1:

How can sentiment analysis be effectively applied to identify prevalent privacy concerns expressed by students using eLearning platforms in higher educational institutions?

Research Objective 1:

Develop a robust sentiment analysis model capable of accurately classifying user responses as positive, or negative in the context of privacy concerns on eLearning platforms.

The first research question aimed to explore the performance of the sentiment analysis model in identifying privacy concerns within student feedback on eLearning platforms. The performance of sentiment analysis in this context lies in its ability to effectively generalize and process large volumes of textual data, such as student reviews, and feedback, and classify them into sentiments (positive or negative). Our sentiment analysis model successfully categorized responses into positive, and negative sentiments, with a particular focus on those associated with privacy issues.

Considering the literature on sentiment analysis in educational contexts such as works by (Onan, 2021). Our findings align with this trend, reinforcing the significance of deep learning-based approaches in educational sentiment analysis. The results from the models suggest that deep learning architectures can capture dependencies in textual data and are effective for classification tasks. This supports,

(Kechaou et al., 2011) that classified a wide range of extracted opinions/sentiments expressed in eLearning platforms. Our sentiment model extracts similar sentiment from the eLearning platforms based on user feedback; however, in contrast, these extracts are based on the security and privacy of the eLearning systems expressed in the opinions of the learners.

Alternatively, (H. Lee et al., 2013) used the findings of their study to the development of a recommendation system that can assist businesses in identifying potential innovative ideas from a vast array of concepts. This novel idea has not yet been explored in eLearning systems to identify the most prevalent privacy issues that may occur in eLearning systems and in advance find possible ways to mitigate them. The sentiment analysis model will help to explore the learner's sentiment on privacy in the learning system, moving on, it will help us build the privacy classifier that will be used to identify the prevalent privacy issues that may occur in the eLearning system. Yet again, this will provide a knowledge base to understand and know the most prevalent privacy issues in the learning systems — which can help identify prospective ways in advance to mitigate privacy issues collected over time. In furtherance, this will help generate innovative ways to ensure the privacy preservation of stakeholders' information on the learning platform. However, for the sentiment model, our focus on privacy concerns introduced additional complexity, as these concerns often involve more subtle and context-specific language compared to general course evaluation studies identified in the literature. Despite these challenges, our model, powered by BERT pre-trained embeddings, achieved a robust accuracy of 70 %. This slight reduction in accuracy,

compared to the MOOC study, and many others in the literature, can be attributed to the specialized nature of our task, which required the model to differentiate between privacy-related sentiments and other types of negative feedback.

In contrast, the use of BERT embeddings in our study provided a more nuanced understanding of privacy-related language, allowing our model to better capture the context and semantics of student feedback. This is consistent with the results reported in the MOOC study, where the LSTM network with GloVe embeddings was shown to excel in capturing the temporal dependencies in sentiment-laden text.

Moreover, while our study focused on privacy concerns, it would be beneficial to apply similar deep learning techniques to other specific aspects of eLearning feedback, such as academic integrity or student engagement, to further validate the generalizability of deep learning models in educational sentiment analysis. (Onan, 2021) employed sentiment analysis on educational data to gather input on resources and learning materials, which yielded insightful information to improve the calibre of learning materials and pinpoint students' learning preferences. In conjunction, our findings demonstrate that the sentiment model is a powerful tool for detecting privacy concerns — as students often express their discomfort with various privacy practices through negative sentiment responses. This will provide insights to enhance effective security and privacy integration into the Higher institution’s business objectives and requirements. That said positive sentiment will serve as appraisal: there are no privacy breaches experienced by the students and negative sentiment will indicate a potential privacy breach and therefore swift action is needed. According to (Baragash et al., 2022), sentiment

and satisfaction indicators in student posts, comments, and feedback, sentiment analysis has the potential to significantly enhance the teaching and learning process in higher education by assisting administrators and instructors in identifying students' trouble spots and taking prompt corrective action. Juxtaposing that to our results, this feedback through the sentiment analysis model will help administrators understand student concerns about their privacy and areas that require prompt actions. The model was particularly adept at identifying dissatisfaction related to data leaks/data breaches, location tracking, and Identity theft issues.

However, the accuracy of the sentiment classification was sometimes compromised by the complexity of the language used by students, suggesting that further refinement of the model, including the integration of contextual analysis, could enhance its effectiveness. This same suggestion was made by (Mukhopadhyay & Singh, 2023) in their study. The ability to automatically classify and flag privacy-related concerns from large volumes of student feedback provides educational institutions with a proactive means of identifying potential issues before they escalate. This will render asunder, the consequences of failing to protect personal and academic data, identified by (Roussos et al., 2023) The higher the Institution and security objectives align, the more successful the two will be. This aligns to develop a robust sentiment analysis model that accurately captures privacy-related sentiments.

4.5 Discussion on Research Question 2

Research Question 2:

What specific privacy issues are commonly raised by students in negative sentiment responses, and how can these issues be addressed through effective privacy preservation measures?

Research Objective 2:

Train a privacy classifier model to identify specific privacy concerns within negative sentiment responses, focusing on issues such as data collection, data breaches, Identity theft, and Location Tracking.

As asserted by (Friedewald et al., 2017), privacy is not a definite issue in that what might be classified as a privacy breach in one instance might not be perceived as a privacy breach in another. We acknowledge that privacy is multifaceted and highly context-based — and requires a comprehensive approach to address them. Therefore, we choose Data leakage, Identity theft, and location tracking as our targets so that we can train our classifier on them. These three privacy breaches above represent diverse and critical aspects of user privacy in digital environments, particularly in eLearning systems. They pose substantial risks to user trust, security, and compliance with privacy regulations.

According to (Chen & He, 2013) the risk increases with the complexity of online learning systems' features and functionalities; hence the scope of the privacy classifier can be expanded to cater for the complexities that may arise as the system

becomes more complex. According to (Al-Hail et al., 2023), learners feel worried about using online learning because of privacy and ethical issues.

This research question addresses this concern by creating awareness and involving the learners in identifying the prevalent privacy issue. This will alleviate the worry about their privacy and ethical issues while we encourage open and shared knowledge on digital platforms. (Prinsloo et al., 2019) suggests that Massive Open Online Courses (MOOCs) are much more interested in protecting their interest, not the users or clients. This research tries to prioritise the users in response to getting feedback from them as to how they feel about their privacy and security on the eLearning systems which helps the administrators further take actions to protect their privacy on the learning system. The second research question sought to identify the specific privacy concerns most frequently expressed by students in negative sentiment responses. Our privacy classifier model, trained on our dataset, can identify the privacy issue within the textual responses from the users of the eLearning system with only a 28% margin of error. Following this, after the responses are collected over time, the most prevalent privacy issues will be noticed and further action can be taken to mitigate those issues.

Moreover, much insight can be gleaned from the response and the choice of the privacy-preserving algorithm can be used to effectively address those issues. (Ivanova et al., 2022) explores the application and necessity of privacy-preserving algorithms in eLearning environments to protect students' identity and data. Assuming that over three months the privacy classifier collates data leakage as the most prevalent privacy breach in the learning system, the most appropriate privacy-

preserving algorithm would be K-Anonymity — replacing specific data with more general representations or t-Closeness algorithm — making sure that the distribution of a sensitive attribute in any k-anonymous group closely resembles the distribution of the attribute in the whole data. Since the majority of entities and organizations prioritize the most important problems and high-risk processing tasks with their limited resources, this will provide an effective system to support human experts in privacy preservation tasks by automating the detection of prevalent privacy issues in the eLearning, rather than relying solely on manual effort by human experts. By doing so, institutions can detect and address privacy concerns more swiftly and accurately. These findings and insight underscore the need for higher educational institutions to focus on these specific areas of privacy breaches when designing and implementing privacy preservation measures. By addressing the concerns identified by the privacy classifier model, institutions can create a safer online learning environment. The research objective of training a privacy classifier model to pinpoint specific privacy issues has been successfully met, as demonstrated by the model's ability to highlight key areas of concern and provide privacy issues within the feedback from the learners.

4.6 Discussion on Research Question 3

Research Question 3:

How can higher educational institutions leverage sentiment analysis and privacy classification models to identify and mitigate privacy issues within their eLearning environments proactively?

Research Objective 3:

Develop recommendations for higher educational institutions to address identified privacy concerns, including implementing appropriate privacy preservation measures and fostering a responsible data handling and transparency culture.

Although the eLearning system's infrastructure and content have been developed with significant effort, very little work has been done to keep the system secure (R. Ali & Zafar, 2017; Bhatia & Maitra, 2018; Kritzinger, 2006). If the sentiment and privacy classifier model are both integrated into the learning systems, it will provide actionable steps for institutions to enhance privacy preservation on their eLearning platforms.

The third research question explored how higher educational institutions can utilize the insights gained from both the sentiment analysis and privacy classification models to manage privacy risks proactively. The possible integration of these models into the privacy management framework of educational institutions offers a novel approach to addressing privacy concerns in eLearning environments. Most of the literature sees student feedback as an important component of the

quality assurance and control process. As such, (He et al., 2015) offered a framework for gathering online public sentiment about a product's reputation. When compared to the traditional survey strategy, they discover that text mining approaches offer both a significantly lower cost and a greater amount of knowledge discovery from public opinion. In light of this, this study through the sentiment and privacy model will be a key benchmark for effective security and privacy breach knowledge discovery. By continuously analyzing student responses, the model could identify shifts in sentiment that may indicate emerging privacy concerns or appraisal. For instance, a noticeable spike in negative sentiment could signal a recent change in platform policy or functionality that students perceive as a threat to their privacy.

In effect, the privacy classifier model goes beyond general sentiment analysis by categorizing specific privacy issues within negative sentiment responses. This capability will allow higher institutions to understand the precise nature of the concerns being raised. For example, if a significant portion of negative feedback is classified under 'identity theft,' the institution can prioritize enhancing its identity verification processes and securing personal data. This detailed level of insight will enable higher institutions to target their interventions more effectively. For example, if location tracking is a frequent concern, the institution might consider providing clearer information about how and why location data is used, or even revising data collection practices to better align with student expectations. Additionally, if the classifier indicates a high frequency of concerns related to data breaches, the institution might prioritize upgrading its cybersecurity measures and

educating students on how their data is protected. In furtherance of technical measures, institutions can also implement educational campaigns to inform students about best practices for safeguarding their privacy. These campaigns can be informed by the data-driven insights from both models, ensuring that they address the most relevant and current concerns.

This proactive approach allows for immediate interventions, such as revising data handling practices or improving security measures, to prevent minor concerns from becoming significant problems. The privacy classification model complements this process by providing detailed insights into the specific nature of the concerns raised, enabling institutions to develop targeted privacy preservation strategies identified earlier, and awareness creation through open interaction with students. As a result, educational institutions and instructors will be better able to respond to and accommodate students' security and privacy concerns as necessary. The findings suggest that by continuously analyzing student feedback through sentiment analysis, Higher Institutions can identify emerging privacy issues in real time. Institutions that actively engage with students about their data policies and privacy measures are likely to build stronger trust and improve overall student satisfaction. Consequently, students will feel supported, more involved, and partially responsible for safeguarding their privacy and security on the eLearning system.

According to (Shang et al., 2021), learners' privacy concerns and trust affect their desire to utilize online learning systems. One of the key benefits of integrating sentiment analysis and privacy classification models into eLearning platforms is

the potential to enhance trust and transparency. When students see that their feedback is being actively monitored and that their concerns are being addressed, they are more likely to trust the platform and feel secure using it. This increased trust can lead to higher levels of engagement and satisfaction, ultimately improving the overall learning experience. Data-driven decisions based on the models' outputs institutions can demonstrate their commitment to student privacy, fostering a culture of transparency and responsible data handling. This not only helps protect students' personal information but also enhances the institution's reputation as a leader in privacy-preserving educational practices. The recommendations developed as part of this research align to provide actionable steps for institutions to enhance privacy preservation on their eLearning platforms. Moreover, the study emphasizes how crucial openness and communication are to developing a culture of ethical data handling.

In all (Nasukawa & Yi, 2003) propose an all-inclusive approach to mitigate privacy issues in the eLearning system. This research is in line with this suggestion as it includes the stakeholders on the learning platform to help shape the privacy and security metrics of the eLearning system. This will also assist higher education institutions in creating an appropriate budget for a security program and the security components that make it up. It will also serve as a useful technique to inform and optimize the application of privacy preservation algorithms like k-anonymity and differential privacy and many others in eLearning learning environments. Upshot for the industry experts, security and privacy training resources can be tailored to

the most prevalent privacy issues instead of holistic security training which might not be cost-effective.

In conclusion, we presented the evaluation of the model's performances using standard metrics such as precision accuracy etc. Moreover, we specified the relevance of the study highlighting the need for higher institutions to prioritize their limited resources to protect against threats that they might be exposed to. As previously mentioned, the answers will entail creating knowledge-based solutions that are bolstered by analyzing student sentiment and forecasting the most common privacy concerns on the eLearning platform. This subtle solution can lead to the integration of Privacy Enhancing Technologies such as identity protection, location tracking, and data security enhancement. This technology will largely strengthen user privacy and secure learning environments. This will again provide adept privacy preserving task within the eLearning system.

CHAPTER FIVE

5.1. Introduction

This chapter will start by summarizing the study's results and limitations before offering suggestions for additional research.

5.2. Summary of the findings

It is tough to construct a knowledge base to identify learners' sentiments on their privacy and further report privacy issues on an online system. This study aimed to ensure privacy preservation in eLearning systems in higher educational institutions. We leveraged the feasibility of using Deep learning algorithms and natural language processing techniques such as sentiment analysis and text classification to ensue privacy preservation on eLearning systems from the perspective of learners. The text classifier model predicts the most prevalent privacy issue on the online learning platform particularly for negative sentiment; with the assumption that negative sentiment might contain some level of privacy breaches. The results from the models indicate 80% and 74% accuracy for the sentiment and text classifier respectively during the testing. This percentage shows how robust both models can generalize unseen data. Other supporting metrics such as F1-score, Confusion Metrics were all used to measure the effectiveness of the models. This model demonstrated remarkable performance with accuracy, precision, recall, and F1-scores of 0.841, 0.850, 0.840, and 0.844, respectively, on our dataset that was identified in the preceding chapters.

The finding appeared to suggest recommendations can be made to enhance privacy and technology integration within the higher educational institution's eLearning environment in the end. As these predictions both the sentiment and the privacy issues are collected over a while, the dominant sentiment and privacy issue can provide insight and recommendation to various ways such as user education, the choice of the privacy-preserving algorithm etc. that can enhance the privacy of the learners in the higher institution. Further, for higher institutions to tailor their limited resources to privacy security awareness training it is imperative to identify the prevalent issues on the learning platform. This will allow effective allocation of the limited resources rather than a holistic approach to creating privacy and security awareness amongst the learners who are patronizing the service of the online learning platform. A subtle objective of this study.

5.3.Contribution

The online learning platforms leverage internet protocols to deliver the information. It evidences the numerous cyber-attacks that occur on the internet hence online learning systems might not be exempted from these scrupulous activities. Various pieces of literature identified focused on the adoption and course evaluation of eLearning systems using the sentiment of learners' textual data. However, in this study, the security and privacy of the learners have been mined to understand various prevalent privacy issues that may exist in the learning platforms. For MOOCs, research shows that the main focus is their content not necessarily the privacy of the users/learner. As a result, this research developed a sentiment analysis and privacy classifier model which expertly combined a deep learning

model with some custom layers. These models serve as a knowledge base to provide various privacy issues in the learning system and the most prevalent privacy breaches that may occur. This knowledge base will serve as a repertoire for prompt actions to be taken for privacy preservation when the privacy breach incident is noticed. Additionally, this will help universities create a budget that is both acceptable and appropriate for a security program and the security components that make it up. It will also be valuable in informing and optimizing the usage of privacy preservation techniques such as k-anonymity, differential privacy, and many others in eLearning learning environments. As a result, industry professionals may customize security and privacy training materials to the most common privacy concerns rather than comprehensive security training, which may be more expensive.

In summary, given the critical importance of internet security, this study aimed to identify potential antecedents of privacy concerns by applying sentiment analysis within the context of eLearning platforms in higher educational institutions. This chapter concluded the study by addressing the research aims and questions, focusing on privacy concerns within eLearning platforms in higher educational institutions. Through sentiment analysis, the study identified key antecedents to these concerns. Specifically, identity theft, data leakage, and location tracking—the primary targets identified by the privacy classification model—were prevalent privacy concerns frequently detected in negative sentiment responses. The model's ability to pinpoint these concerns highlights its effectiveness in analyzing student feedback on eLearning platforms. Based on these findings,

actionable recommendations were developed to help educational institutions proactively address these concerns by implementing robust privacy-preserving measures. The chapter also reviewed the limitations of the sentiment analysis and privacy classification models, such as their scope and generalizability. These limitations provided a foundation for future research recommendations, including expanding the model to capture additional privacy concerns and applying the findings in a broader range of eLearning systems.

5.4.Limitations

As identified in the previous chapters, this research focused solely on selected higher institutions. This limited sample size may not be sufficient to generalize any hypotheses. Furthermore, in sentiment analysis, sarcasm can be interpreted differently by humans, whereas machines struggle to recognize it. This presents a significant challenge for researchers in the natural language processing domain. Another noteworthy phenomenon encountered in this study involves the unique challenges associated with mining e-learning reviews and analyzing e-learning blogs, which complicates the task and contributes to its complexity. This factor was a primary cause of our loss of accuracy. It is important to note that this research does not explicitly aim to address the issue of privacy in eLearning platforms. However, as previously mentioned, it will serve as a knowledge base to assist researchers, industry experts, and product designers in better understanding the prevalent privacy concerns and student sentiments regarding their privacy within learning systems. This insight will facilitate a tailored and comprehensive approach to ensure privacy preservation in the eLearning platform.

5.5.Recommendation

Future research should explore the application of other pre-trained models, such as GPT-4, alongside various word embedding techniques like GloVe and Word2Vec, within deep learning architectures for discovering user sentiment and privacy issues, as well as recommendations for improving results. Furthermore, the study could be expanded to encompass a wider context, targeting higher education institutions nationwide. All stakeholders within the institution should be included in the research rather than relying solely on the selected samples from this study. Since the BERT pre-trained model and its associated word embeddings, WordPiece, were utilized in this research, future work could incorporate different deep learning models, including RoBERTa and LSTM. Additionally, privacy classifiers can be broadened in subsequent studies to encompass a wider range of privacy issues within the eLearning system. Consequently, institutions could investigate the integration of these models into more extensive data governance frameworks. This would not only involve monitoring student feedback but also integrating other data sources, such as system logs and third-party evaluations, to offer a more comprehensive understanding of privacy risks. Moreover, as the fields of NLP and deep learning continue to advance, institutions may find it beneficial to update their models to take advantage of the latest developments, ensuring that their privacy monitoring capabilities remain cutting-edge.

REFERENCES

Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999). Privacy in e-commerce: examining user scenarios and privacy preferences. *Proceedings of the 1st ACM Conference on Electronic Commerce*, 1–8.

Ahmed, S., Buragga, K., & Ramani, A. K. (2011). Security issues concern for E-Learning by Saudi universities. *13th International Conference on Advanced Communication Technology (ICACT2011)*, 1579–1582.

Aïmeur, E., Hage, H., & Mani Onana, F. S. (2007). A framework for privacy-preserving e-learning. *Trust Management: Proceedings of IFIPTM 2007: Joint ITrust and PST Conferences on Privacy, Trust Management and Security, July 30–August 2, 2007, New Brunswick, Canada 1*, 223–238.

Alatrista-Salas, H., Cordero, H., & Nunez-del-Prado, M. (2019). PS I Love You: Privacy Aware Sentiment Classification. *Computación y Sistemas*, *23*(4), 1507–1515.

Aldheleai, H. F., Bokhari, M. U., & Hamatta, H. S. A. (2015). User security in e-learning system. *2015 Fifth International Conference on Communication Systems and Network Technologies*, 767–770.

Al-Hail, M., Zguir, M. F., & Koç, M. (2023). University students' and educators' perceptions on the use of digital and social media platforms: A sentiment analysis and a multi-country review. *Iscience*, *26*(8).

Ali, M. M. (2021). Arabic sentiment analysis about online learning to mitigate covid-19. *Journal of Intelligent Systems*, *30*(1), 524–540.

Ali, R., & Zafar, H. (2017). A security and privacy framework for e-Learning. *International Journal for E-Learning Security*.

Alier, M., Casany, M. J., Severance, C., & Amo, D. (2020). Learner Privacy, a pending assignment. *Eighth International Conference on Technological Ecosystems for Enhancing Multiculturality*, 725–729.

Alkhodair, S. A. (2023). A SENTIMENT ANALYSIS-BASED SMARTPHONE APPLICATION TO CONTINUOUSLY ASSESS STUDENTS'FEEDBACK AND MONITOR THE QUALITY OF COURSES AND THE LEARNING EXPERIENCE IN EDUCATIONAL INSTITUTIONS. *IJAEDU-International E-Journal of Advances in Education*, *9*(25), 15–26.

Alnasser, W., Beigi, G., & Liu, H. (2021). Privacy preserving text representation learning using bert. *Social, Cultural, and Behavioral Modeling: 14th International Conference, SBP-BRiMS 2021, Virtual Event, July 6–9, 2021, Proceedings 14*, 91–100.

AL-Rubaiee, H. S., Qiu, R., Alomar, K., & Li, D. (2016). *Sentiment analysis of Arabic tweets in e-learning*.

Azemović, J. (2012). Privacy aware eLearning environments based on hippocratic database principles. *Proceedings of the Fifth Balkan Conference in Informatics*, 142–149.

Baker, H., Hallowell, M. R., & Tixier, A. J.-P. (2020). Automatically learning construction injury precursors from text. *Automation in Construction*, *118*, 103145.

Balahadia, F. F., Fernando, M. C. G., & Juanatas, I. C. (2016). Teacher's performance evaluation tool using opinion mining with sentiment analysis. *2016 IEEE Region 10 Symposium (TENSYMP)*, 95–98.

Baragash, R. S., Aldowah, H., & Umar, I. N. (2022). Students' Perceptions of E-Learning in Malaysian Universities: Sentiment Analysis Based Machine Learning Approach. *J. Inf. Technol. Educ. Res.*, *21*, 439–463.

Basu, P., Roy, T. S., Naidu, R., & Muftuoglu, Z. (2021). Privacy enabled financial text classification using differential privacy and federated learning. *ArXiv Preprint ArXiv:2110.01643*.

Besmer, A. R., Watson, J., & Banks, M. S. (2020). Investigating user perceptions of mobile app privacy: An analysis of user-submitted app reviews. *International Journal of Information Security and Privacy (IJISP)*, *14*(4), 74–91.

Bhatia, M., & Maitra, J. K. (2018). E-learning platforms security issues and vulnerability analysis. *2018 International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES)*, 276–285.

Blackmon, S. J., & Major, C. H. (2023). Inclusion or infringement? A systematic research review of students' perspectives on student privacy in technology-enhanced, hybrid and online courses. *British Journal of Educational Technology*, *54*(6), 1542–1565.

Borcea, K., Donker, H., Franz, E., Pfitzmann, A., & Wahrig, H. (2006). Towards privacy-aware elearning. *Privacy Enhancing Technologies: 5th International Workshop, PET 2005, Cavtat, Croatia, May 30-June 1, 2005, Revised Selected Papers 5*, 167–178.

Borcea-Pfitzmann, K., & Stange, A.-K. (2007). Privacy-an Issue for eLearning? A Trend Analysis Reflecting the Attitude of European eLearning Users. *ArXiv Preprint ArXiv:0705.0612*.

Buccafurri, F., Fotia, L., Lax, G., & Saraswat, V. (2016). Analysis-preserving protection of user privacy against information leakage of social-network Likes. *Information Sciences*, *328*, 340–358.

Chang, B. (2021). Student privacy issues in online learning environments. *Distance Education*, *42*(1), 55–69.

Chaplot, D. S., Rhim, E., & Kim, J. (2015). Predicting Student Attrition in MOOCs using Sentiment Analysis and Neural Networks. *AIED Workshops*, *53*, 54–57.

Chen, Y., & He, W. (2013). Security risks and protection in online learning: A survey. *International Review of Research in Open and Distributed Learning*, *14*(5), 108–127.

Chou, H.-L., & Chen, C.-H. (2016). Beyond identifying privacy issues in e-learning settings–Implications for instructional designers. *Computers & Education*, *103*, 124–133.

Colace, F., De Santo, M., & Greco, L. (2014). SAFE: A Sentiment Analysis Framework for E-Learning. *International Journal of Emerging Technologies in Learning*, *9*(6).

Derawi, M. (2014). Securing e-learning platforms. *2014 International Conference on Web and Open Access to Learning (ICWOAL)*, 1–4.

Ding, W. (2019). Low-dimensional vectors with density bounded by 5/6 are pinwheel schedulable. *Algorithmic Aspects in Information and Management: 13th International Conference, AAIM 2019, Beijing, China, August 6–8, 2019, Proceedings 13*, 51–61.

Dolianiti, F. S., Iakovakis, D., Dias, S. B., Hadjileontiadou, S., Diniz, J. A., & Hadjileontiadis, L. (2018). Sentiment analysis techniques and applications in education: A survey. *International Conference on Technology and Innovation in Learning, Teaching and Education*, 412–427.

Ergen, T., Sahiner, A., Ozturkler, B., Pauly, J., Mardani, M., & Pilanci, M. (2021). Demystifying batch normalization in relu networks: Equivalent convex optimization models and implicit regularization. *ArXiv Preprint ArXiv:2103.01499*.

Escotet, M. Á. (2023). The optimistic future of Artificial Intelligence in higher education. *Prospects*, 1–10.

Estrada, M. L. B., Cabada, R. Z., Bustillos, R. O., & Graff, M. (2020). Opinion mining and emotion recognition applied to learning environments. *Expert Systems with Applications*, *150*, 113265.

Feng, X., Wei, Y., Pan, X., Qiu, L., & Ma, Y. (2020). Academic emotion classification and recognition method for large-scale online learning environment—Based on A-CNN and LSTM-ATT deep learning pipeline method. *International Journal of Environmental Research and Public Health*, *17*(6), 1941.

Fourure, D., Javaid, M. U., Posocco, N., & Tihon, S. (2021). Anomaly detection: How to artificially increase your f1-score with a biased evaluation protocol. *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*, 3–18.

Friedewald, M., Burgess, J. P., Čas, J., Bellanova, R., & Peissl, W. (2017). *Surveillance, privacy and security*. Taylor & Francis.

Gkontzis, A. F., Karachristos, C. V, Panagiotakopoulos, C. T., Stavropoulos, E. C., & Verykios, V. S. (2017). Sentiment analysis to track emotion and polarity in student fora. *Proceedings of the 21st Pan-Hellenic Conference on Informatics*, 1–6.

Goutte, C., & Gaussier, E. (2005). A probabilistic interpretation of precision, recall and F-score, with implication for evaluation. *European Conference on Information Retrieval*, 345–359.

Gunasekaran, K. P. (2023). Exploring sentiment analysis techniques in natural language processing: A Comprehensive Review. *ArXiv Preprint ArXiv:2305.14842*.

Hasan, S. H., Alghazzawi, D. M., & Zafar, A. (2014). E-Learning systems and their Security. *BRIS Journal of Adv. S & T (ISSN. 0971-9563) Vol*, *2*, 83–92.

He, W., Wu, H., Yan, G., Akula, V., & Shen, J. (2015). A novel social media competitive analytics framework with sentiment benchmarks. *Information & Management*, *52*(7), 801–812.

Hilmi, M. F., & Mustapha, Y. (2022). Perceived Security of E-Learning Portal. *ArXiv Preprint ArXiv:2209.11196*.

Humphreys, L., Gill, P., & Krishnamurthy, B. (2010). How much is too much? Privacy issues on Twitter. *Conference of International Communication Association, Singapore*.

Idrees, S. M., & Nowostawski, M. (2024). *Blockchain Transformations: Navigating the Decentralized Protocols Era*. Springer Nature Switzerland, Imprint: Springer.

Ivanova, M., Trifonova, I., & Bogdanova, G. (2022). Privacy Preservation in eLearning: Exploration and Analysis. *2022 20th International Conference on Information Technology Based Higher Education and Training (ITHET)*, 1–8.

Jim, J. R., Talukder, M. A. R., Malakar, P., Kabir, M. M., Nur, K., & Mridha, M. F. (2024). Recent advancements and challenges of nlp-based sentiment analysis: A state-of-the-art review. *Natural Language Processing Journal*, 100059.

Joseph, J., Vineetha, S., & Sobhana, N. V. (2022). A survey on deep learning based sentiment analysis. *Materials Today: Proceedings*, *58*, 456–460.

Kamp, J., Beinborn, L., & Fokkens, A. (2022). Perturbations and subpopulations for testing robustness in token-based argument unit recognition. *ArXiv Preprint ArXiv:2209.14780*.

Kastrati, Z., Dalipi, F., Imran, A. S., Pireva Nuci, K., & Wani, M. A. (2021). Sentiment analysis of students' feedback with NLP and deep learning: A systematic mapping study. *Applied Sciences*, *11*(9), 3986.

Kechaou, Z., Ammar, M. Ben, & Alimi, A. M. (2011). Improving e-learning with sentiment analysis of users' opinions. *2011 IEEE Global Engineering Education Conference (EDUCON)*, 1032–1038.

Khan, L., Amjad, A., Afaq, K. M., & Chang, H.-T. (2022). Deep sentiment analysis using CNN-LSTM architecture of English and Roman Urdu text shared in social media. *Applied Sciences*, *12*(5), 2694.

Kharbat, F. F., & Abu Daabes, A. S. (2021). E-proctored exams during the COVID-19 pandemic: A close understanding. *Education and Information Technologies*, *26*(6), 6589–6605.

Khurana, D., Koli, A., Khatter, K., & Singh, S. (2023). Natural language processing: State of the art, current trends and challenges. *Multimedia Tools and Applications*, *82*(3), 3713–3744.

Kim, S. S. (2023). Motivators and concerns for real-time online classes: focused on the security and privacy issues. *Interactive Learning Environments*, *31*(4), 1875–1888.

Kritzinger, E. (2006). Information Security in an E-learning Environment. *Education for the 21st Century—Impact of ICT and Digital Resources: IFIP 19th World Computer Congress, TC-3, Education, August 21–24, 2006, Santiago, Chile*, 345–349.

Laksana, E. A., Suryana, A., Rosita, A., & Heryono, H. (2018). Evaluation of E-learning Activity Effectiveness in Higher Education Through Sentiment Analysis by Using Naïve Bayes Classifier. *Sisforma*, *5*(1), 22.

Le, K., Luong-Ha, N., Nguyen-Duc, M., Le-Phuoc, D., Do, C., & Wong, K.-S. (2024). Exploring the Practicality of Federated Learning: A Survey Towards the Communication Perspective. *ArXiv Preprint ArXiv:2405.20431*.

Lee, C. B., Io, H. N., & Tang, H. (2022). Sentiments and perceptions after a privacy breach incident. *Cogent Business & Management*, *9*(1), 2050018.

Lee, G., Kim, M., Park, J. H., Hwang, S., & Cheon, J. H. (2022). Privacy-preserving text classification on BERT embeddings with homomorphic encryption. *ArXiv Preprint ArXiv:2210.02574*.

Lee, H., Choi, K., Yoo, D., Suh, Y., He, G., & Lee, S. (2013). *The more the worse? Mining valuable ideas with sentiment analysis for idea recommendation*.

Li, X., & Pei, Z. (2023). Improving effectiveness of online learning for higher education students during the COVID-19 pandemic. *Frontiers in Psychology*, *13*, 1111028.

Li, Y., Pan, Q., Yang, T., Wang, S., Tang, J., & Cambria, E. (2017). Learning word representations for sentiment analysis. *Cognitive Computation*, *9*, 843–851.

Lin, N. H., Korba, L., Yee, G., Shih, T. K., & Lin, H. W. (2004). Security and privacy technologies for distance education applications. *18th International Conference on Advanced Information Networking and Applications, 2004. AINA 2004.*, *1*, 580–585.

Mahendran, D., Luo, C., & Mcinnes, B. T. (2021). Privacy-preservation in the context of natural language processing. *IEEE Access*, *9*, 147600–147612.

Majeed, A., Baadel, S., & Haq, A. U. (2016). Global triumph or exploitation of security and privacy concerns in e-learning systems. *Global Security, Safety and Sustainability-The Security Challenges of the Connected World: 11th International Conference, ICGS3 2017, London, UK, January 18-20, 2017, Proceedings 11*, 351–363.

Mandal, L., Das, R., Bhattacharya, S., & Basu, P. N. (2017). Intellimote: a hybrid classifier for classifying learners' emotion in a distributed e-learning

environment. *Turkish Journal of Electrical Engineering and Computer Sciences*, *25*(3), 2084–2095.

Martinelli, F., Marulli, F., Mercaldo, F., Marrone, S., & Santone, A. (2020). Enhanced privacy and data protection using natural language processing and artificial intelligence. *2020 International Joint Conference on Neural Networks (IJCNN)*, 1–8.

May, M., & George, S. (2011). Using students' tracking data in e-learning: Are we always aware of security and privacy concerns? *2011 IEEE 3rd International Conference on Communication Software and Networks*, 10–14.

Mehdy, A. K., & Mehrpouyan, H. (2020). A user-centric and sentiment aware privacy-disclosure detection framework based on multi-input neural network. *The PrivateNLP 2020 Workshop on Privacy and Natural Language Processing Colocated with 13th ACM International WSDM Conference, 2020, in Houston, Texas, USA.*

Mehta, M., De, S. J., & Chattopadhyay, M. (2022). Elucidating the role of emotion in privacy-concerns: A text-Convolutional Neural Network (text-CNN)-based tweets analysis of contact tracing apps. *Australasian Journal of Information Systems*, *26*.

Mikolov, T., Sutskever, I., Chen, K., Corrado, G. S., & Dean, J. (2013). Distributed representations of words and phrases and their compositionality. *Advances in Neural Information Processing Systems*, *26*.

Moon, S., Chi, S., & Im, S.-B. (2022). Automated detection of contractual risk clauses from construction specifications using bidirectional encoder representations from transformers (BERT). *Automation in Construction*, *142*, 104465.

Mujahid, M., Lee, E., Rustam, F., Washington, P. B., Ullah, S., Reshi, A. A., & Ashraf, I. (2021). Sentiment analysis and topic modeling on tweets about online education during COVID-19. *Applied Sciences*, *11*(18), 8438.

Mukhopadhyay, S., & Singh, M. (2023). Student Emotional Complexity Analysis with NLP and Machine Learning in Educational Contexts. *2023 OITS International Conference on Information Technology (OCIT)*, 648–654.

Mustapha, M., Krasnashchok, K., Al Bassit, A., & Skhiri, S. (2020). Privacy policy classification with xlnet (short paper). *International Workshop on Data Privacy Management*, 250–257.

Mutimukwe, C., Viberg, O., Oberg, L., & Cerratto-Pargman, T. (2022). Students' privacy concerns in learning analytics: Model development. *British Journal of Educational Technology*, *53*(4), 932–951.

Nasukawa, T., & Yi, J. (2003). Sentiment analysis: Capturing favorability using natural language processing. *Proceedings of the 2nd International Conference on Knowledge Capture*, 70–77.

Newman, H., & Joyner, D. (2018). Sentiment analysis of student evaluations of teaching. *Artificial Intelligence in Education: 19th International Conference,*

AIED 2018, London, UK, June 27–30, 2018, Proceedings, Part II 19, 246–250.

Onan, A. (2019). Deep learning based sentiment analysis on product reviews on Twitter. *Big Data Innovations and Applications: 5th International Conference, Innovate-Data 2019, Istanbul, Turkey, August 26–28, 2019, Proceedings 5*, 80–91.

Onan, A. (2021). Sentiment analysis on massive open online course evaluations: a text mining and deep learning approach. *Computer Applications in Engineering Education*, *29*(3), 572–589.

Ortigosa, A., Martín, J. M., & Carro, R. M. (2014). Sentiment analysis in Facebook and its application to e-learning. *Computers in Human Behavior*, *31*, 527–541.

Pathak, A. R., Pandey, M., & Rautaray, S. (2021). Topic-level sentiment analysis of social media data using deep learning. *Applied Soft Computing*, *108*, 107440.

Pekárek, M., & Pötzsch, S. (2009). A comparison of privacy issues in collaborative workspaces and social networks. *Identity in the Information Society*, *2*, 81–93.

Pennington, J., Socher, R., & Manning, C. D. (2014). Glove: Global vectors for word representation. *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, 1532–1543.

Persada, S., Oktavianto, A., Miraja, B., Nadlifatin, R., Belgiawan, P., & Redi, A. A. N. P. (2020). Public perceptions of online learning in developing countries: A study using the ELK stack for sentiment analysis on Twitter. *International Journal of Emerging Technologies in Learning (IJET)*, *15*(9), 94–109.

Prasad, S. B. A., & Nakka, R. P. K. (2023). Supervised Sentiment Analysis of Indirect Qualitative Student Feedback for Unbiased Opinion Mining. *Engineering Proceedings*, *59*(1), 15.

Prinsloo, P., Slade, S., & Khalil, M. (2019). Student data privacy in MOOCs: A sentiment analysis. *Distance Education*, *40*(3), 395–413.

Qazi, A., Raj, R. G., Hardaker, G., & Standing, C. (2017). A systematic literature review on opinion types and sentiment analysis techniques: Tasks and challenges. *Internet Research*, *27*(3), 608–630.

Qureshi, I. A., Ilyas, K., Yasmin, R., & Whitty, M. (2012). Challenges of implementing e-learning in a Pakistani university. *Knowledge Management & E-Learning*, *4*(3), 310.

Raitman, R., Ngo, L., Augar, N., & Zhou, W. (2005). Security in the online e-learning environment. *Fifth IEEE International Conference on Advanced Learning Technologies (ICALT'05)*, 702–706.

Reidenberg, J. R., & Schaub, F. (2018). Achieving big data privacy in education. *Theory and Research in Education*, *16*(3), 263–279.

Roussos, G., Charidimou, D., & Agorogianni, A. (2023). Using SaaS in a European University: Protect your Privacy and enjoy! *Proceedings of European University*, *95*, 27–36.

Sangaroonsilp, P., Choetkiertikul, M., Dam, H. K., & Ghose, A. (2023). An empirical study of automated privacy requirements classification in issue reports. *Automated Software Engineering*, *30*(2), 20.

Saura, J. R., Palacios-Marqués, D., & Ribeiro-Soriano, D. (2021). Using data mining techniques to explore security issues in smart living environments in Twitter. *Computer Communications*, *179*, 285–295.

Sennrich, R., Haddow, B., & Birch, A. (2015). Neural machine translation of rare words with subword units. *ArXiv Preprint ArXiv:1508.07909*.

Sethi, M., Pandey, S., Trar, P., & Soni, P. (2020). Sentiment identification in COVID-19 specific tweets. *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, 509–516.

Shang, C., Zhao, L., Zheng, Y., & Liu, L. (2021). Study on the Influence of Learners' Trust and Privacy Concerns on the Willingness to Use Online Learning Platforms. *2021 International Conference on Big Data, Artificial Intelligence and Risk Management (ICBAR)*, 163–167.

Silva, P., Gonçalves, C., Godinho, C., Antunes, N., & Curado, M. (2020). Using nlp and machine learning to detect data privacy violations. *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 972–977.

Singh, M., Adebayo, S. O., Saini, M., & Singh, J. (2021). Indian government E-learning initiatives in response to COVID-19 crisis: A case study on online learning in Indian higher education system. *Education and Information Technologies*, *26*(6), 7569–7607.

Singh, P. K., & Husain, M. S. (2014). Methodological study of opinion mining and sentiment analysis techniques. *International Journal on Soft Computing*, *5*(1), 11.

Slade, S., Prinsloo, P., & Khalil, M. (2019). Learning analytics at the intersections of student trust, disclosure and benefit. *Proceedings of the 9th International Conference on Learning Analytics & Knowledge*, 235–244.

Slusky, L. (2020). Cybersecurity of online proctoring systems. *Journal of International Technology and Information Management*, *29*(1), 56–83.

Smrz, P. (2004). Integrating natural language processing into e-learning-A case of Czech. *Proceedings of the Workshop on ELearning for Computational Linguistics and Computational Linguistics for ELearning*, 1–10.

Tang, D., Qin, B., & Liu, T. (2015). Deep learning for sentiment analysis: successful approaches and future challenges. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *5*(6), 292–303.

Tunstall, L., Von Werra, L., & Wolf, T. (2022). *Natural language processing with transformers*. " O'Reilly Media, Inc."

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. *Advances in Neural Information Processing Systems*, *30*.

Waheeb, S. A., Khan, N. A., & Shang, X. (2022). Topic modeling and sentiment analysis of online education in the covid-19 era using social networks based datasets. *Electronics*, *11*(5), 715.

Wang, A., Singh, A., Michael, J., Hill, F., Levy, O., & Bowman, S. R. (2018). GLUE: A multi-task benchmark and analysis platform for natural language understanding. *ArXiv Preprint ArXiv:1804.07461*.

Wang, S., Li, B. Z., Khabsa, M., Fang, H., & Ma, H. (2020). Linformer: Self-attention with linear complexity. *ArXiv Preprint ArXiv:2006.04768*.

Xiao, L., Guo, F.-P., & Lu, Q.-B. (2018). Mobile personalized service recommender model based on sentiment analysis and privacy concern. *Mobile Information Systems*, *2018*.

Xu, J., Ruan, Y., Bi, W., Huang, G., Shi, S., Chen, L., & Liu, L. (2023). On synthetic data for back translation. *ArXiv Preprint ArXiv:2310.13675*.

Xu, S., Barbosa, S. E., & Hong, D. (2020). Bert feature based model for predicting the helpfulness scores of online customers reviews. *Advances in Information and Communication: Proceedings of the 2020 Future of Information and Communication Conference (FICC), Volume 2*, 270–281.

Xu, S., Zhang, C., & Hong, D. (2022). BERT-based NLP techniques for classification and severity modeling in basic warranty data study. *Insurance: Mathematics and Economics*, *107*, 57–67.

Yong, J. (2007). Digital identity design and privacy preservation for e-learning. *2007 11th International Conference on Computer Supported Cooperative Work in Design*, 858–863.

Yong, J. (2008). Enhancing the privacy of e-learning systems with alias and anonymity. *Computer Supported Cooperative Work in Design IV: 11th International Conference, CSCWD 2007, Melbourne, Australia, April 26-28, 2007. Revised Selected Papers 11*, 534–544.

Yong, J. (2011). Security and privacy preservation for mobile e-learning via digital identity attributes. *Journal of Universal Computer Science*, *17*(2), 296–310.

Yussiff, A.-S., Yussiff, A.-L., & Abdulkadir, S. J. (2013). *Internet privacy: A survey of cyber abuses and policy improvements in Ghana*.

Zhang, D., Ye, R., Ko, T., Wang, M., & Zhou, Y. (2023). Dub: Discrete unit back-translation for speech translation. *ArXiv Preprint ArXiv:2305.11411*.

Zhang, L., Wang, S., & Liu, B. (2018). Deep learning for sentiment analysis: A survey. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *8*(4), e1253.