CYBERSECURITY AWARENESS IN ONLINE EDUCATION A CASE STUDY ANALYSIS

MRS.B.SUNITHA DEVI[1], CHILUKA PAVANI[2], CHANDUPATLA SAI KRUTHI [3], B.SWATHI[4]

ASSISTANT PROFESSOR[1], UG SCHOLAR[2,3&4]

DEPARTMENT OF CSE, CMR INSTITUTE OF TECHNOLOGY, KANDLAKOYA VILLAGE, MEDCHAL RD, HYDERABAD, TELANGANA 501401

ABSTRACT— This study examines how well-versed Kyrgyz-Turkish Manas School students are in cybersecurity through online learning. An first-year, second-year, and PhD sample of 517 students from all of the university's faculties participated in the study. Despite the fact that there are a great deal of cyberattacks happening all over the world, our research reveals that the pupils had no knowledge of cybersecurity or the overall effects of assaults. By focusing on issues pertaining to harmful software, safe passwords, and social media security, an analysis of understanding of cybersecurity was conducted. It has been discovered that students' knowledge of cybersecurity is lacking, despite the fact that we live in a technologically advanced age where every aspect of our lives is connected to the net through distance learning. More study has led to the conclusion that security instruction should be provided to students in order to shield them from hacks and improve their use of the web.

Index Terms— CyberSecurity, A Case Study, Online Education, Students..

I. INTRODUCTION

Cyber security has started to become extremely important in both individuals and states alike due to the growth of tech and the infiltration of cyberspace into every area of daily life. Although these advances have made our lives easier, the rise in cyberattacks has necessitated the adoption. The usage of laptops in attacks has not changed. Crimes are defined in this sense as crimes carried out on computers. in the US Bureau of Justice, a cybercrime is any violation of the law that requires computer technology of security measures. The forms of cyberattacks, or the harmful use of the internet age, have altered over the past 20 years, which is another key point. This has caused authors to use new "cyber" terms and risks. Hathaway and colleagues describe a cyberattack as "any step taken to undermine the operation of a computer networks for a political or national security purpose." The most fundamental inquiry to make is, "Does this term accurately define cyberattacks in the modern era?" Saying that hacks are exclusively conducted for political reasons is no longer sufficient when attempting to figure out the nature of cyberattacks. This is due to the evolution of new cyber concepts that have altered the character of cyberattacks knowledge for its commission, investigation, or prosecution. One the one hand, it's critical to define cyber security. The International Telecommunications Union (ITU) defines cyber security as a collection of tools, policies, security concepts, security protects, rules, risk-taking approaches, actions, training, best practises, assurance, and technologies that can be used to protect an organization's and user's assets in the cyberspace, despite the fact that there is no universal definition for the term. In order to protect an organization's and user's assets from relevant security dangers in the cyber environment, cyber security aims to achieve and maintain their security properties.

II. LITERATURE SURVEY

A) "The role of individual learning attitudes and goals in Students' application of information skills in Malaysia," Creative Educ., vol. 6, no. 18, pp. 2002–2012, 2015. A. A. Karim, P. M. Shah, F. Khalid, M. Ahmad, and R. Din.

This study examines how well-versed Kyrgyz-Turkish Manas University students are in cybersecurity through online learning. An college, graduate, and PhD sample of 517 people from all of the university's faculties participated in the study. Despite the fact that there are a great deal of cyberattacks happening all over the world, our research reveals that the pupils had no interest in cybersecurity or the overall effects of cyberattacks. By focusing on issues pertaining to harmful software, safe passwords, and social media security, an analysis of understanding of cybersecurity was conducted. It has been discovered that students' knowledge of cybersecurity is lacking, despite the fact that we live in a technologically advanced age where every aspect of our lives is connected to the internet through distance learning.

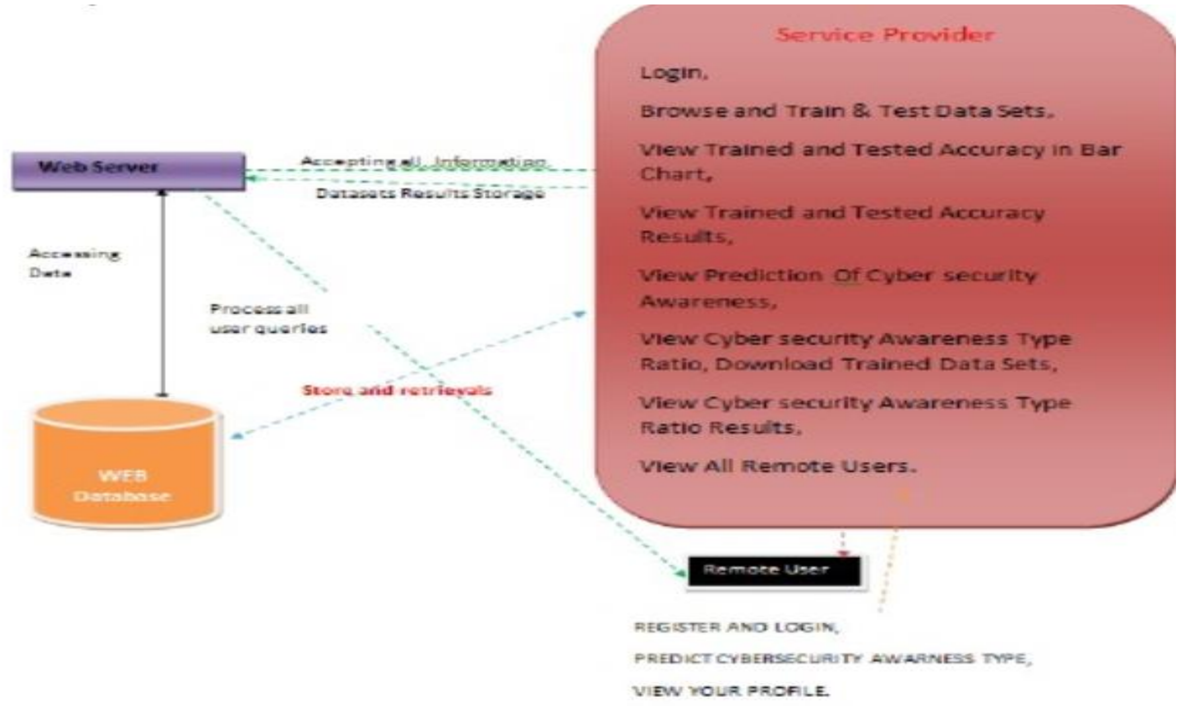
B) "The AI-based cyber threat landscape: A survey," N. Kaloudi and J. Li, ACM Comput. Surv., vol. 53, no. 1,
pp. 1_34, Jan. 2021.

This study measures the level of cybersecurity knowledge attained by Kyrgyz-Turkish Manas college pupils through distance learning. A total of 517 college, master's, and PhD students from all of the university's faculties made up the sample for the study. Our study's findings demonstrate that students' lack of awareness about cybersecurity and the overall effects of cyberattacks is despite the fact that there are numerous cyberattacks taking place all over the world. By focusing on hazardous software, secure passwords, and social media safety questions about cybersecurity knowledge were put together. As COVID-19 took hold and groups and classrooms all over the world had to close their doors, online learning started to become the standard.

C) "A review of emerging threats in cybersecurity," J. Comput. Syst. Sci., vol. 80, no. 5, pp. 973–993, August 2014. J. Jang-Jaccard and S. Nepal.

This paper examines As of April 2020, 186 countries and more than 1.2 billion students were affected by educational institution closures. The school system there has also changed as a result of this pandemic. Online learning is becoming more popular both academics and students because to free and distance learning platforms. The cognitive computing and human intelligence revolution is known as "education 5.0." The main obstacle that one will encounter as the world moves in this direction is how to deal with the risks involved with safety online in the digital age. In order to protect against hacker attacks online, information security awareness might be crucial. The main objective of this paper is to analyse the level of information security awareness, associated risks, and overall effect on the institutions among professors, researchers, freshmen, and employees in schools in the Middle East. The findings show that those polled lack the necessary knowledge and comprehension of the significance of information security concepts and how they are used in their daily job. The Web is becoming a more integral part of many people's, organisations', and countries' daily lives. It has, in large part, positively impacted how people speak. Additionally, it has set up novel business possibilities and given countries the chance to conduct their governments online. Cyber comes with a lot of risks even if it provides an unending array of services and opportunities.

III.PROPOSED SYSTEM


Service Provider
Login,
Browse and Train & Test Data Sets,
View Trained and Tested Accuracy in Bar Chart,
View Trained and Tested Accuracy Results,
View Prediction Of Cyber security Awareness,
View Cyber security Awareness Type Ratio, Download Trained Data Sets,
View Cyber security Awareness Type Ratio Results,
View All Remote Users.
Web Server
Accepting all Information
Datasets Results Storage
Accessing Data
Process all user queries
Store and retrievals
WEB Database
Remote User
REGISTER AND LOGIN,
PREDICT CYBERSECURITY AWARNESS TYPE,
VIEW YOUR PROFILE.

Modules

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Login, Browse Data Sets and Train & Test, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View All Antifraud Model for Internet Loan Prediction, Find Internet Loan Prediction Type Ratio, View Primary Stage Diabetic Prediction Ratio Results, Download Predicted Data Sets, View All Remote Users.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user’s details such as, user name, email, address and admin authorizes the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT PRIMARY STAGE DIABETIC STATUS, VIEW YOUR PROFILE.

CONCLUSION

When the survey findings from students at Kyrgyz Turkish Manas University were analysed, it became clear that the majority of the participants lacked adequate awareness of internet use and cyber threats. They were also discovered to lack technical expertise on a variety of topics, such as what the sites they visit have secure certificates and whether a hacker might get their information by tricking them. It would not be proper to deliver this knowledge exclusively in the parts that provide technical education, as cyber dangers affect those of all educational backgrounds. The findings of this study also demonstrate that those who received cyber security instruction had greater proficiency in computer usage and fundamental network security topics.

REFERENCES

[1] "The role of individual learning attitudes and goals in Students' application of information skills in Malaysia," Creative Educ., vol. 6, no. 18, pp. 2002–2012, 2015. A. A. Karim, P. M. Shah, F. Khalid, M. Ahmad, and R. Din.

[2] "The AI-based cyber threat landscape: A survey," N. Kaloudi and J. Li, ACM Comput. Surv., vol. 53, no. 1,
pp. 1_34, Jan. 2021.

[3] "A review of emerging threats in cybersecurity," J. Comput. Syst. Sci., vol. 80, no. 5, pp. 973–993, August 2014. J. Jang-Jaccard and S. Nepal.

[4] G. Pogrebna and M. Skilton, Navigating New Cyber Risks: How Businesses Can Plan, Build, and Control Safe Spaces in the Digital Age, Palgrave Macmillan, London, U.K., 25 June 2019.

[5] The law of cyber-attack, by O. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, and J. Spiegel, California Law Review, vol. 100, no. 4, 817-885, 2012.

[6] Computer Ethics by F. Forester and P. Morrison. United States: Cambridge, MA: MIT Press, 2001.

[7] Parker, D. 1989. Legal Resource Manual on Digital Crime. The 2nd of January 2022. [Online]. It is possible to get it at https://www.ncjrs.gov/pdf_les1/Digitization/118214NCJRS.pdf.

[8] "Cybersecurity Awareness, Knowledge and Behaviour: A Global Perspective" by M. Zwilling, G. Klien, D. Lesjak,.. Wiechetek, F. Cetin, and H. N. Basim J. Comput. Inf. Syst., vol. 62, no. 1, Jan. 2022, pp. 82–97, "comparative study."