SJIF Impact Factor (2023): 8.574| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 8 | Issue: 10 | October 2023 - Peer Reviewed Journal

EVOLVING LANDSCAPE OF CYBERSECURITY SKILLS: AN ANALYSIS OF SKILL REQUIREMENTS AND GAPS IN KERALA

Jais Binoy
Research Associate, International Centre for Technological Innovations, Kerala.

ABSTRACT

This comprehensive study delves into the dynamic landscape of cybersecurity education and career development within the context of Kerala, India. It addresses a fundamental research question: What are the essential skills and knowledge areas required for various roles within cybersecurity, and how do these requirements vary among roles? Furthermore, it explores emerging skills vital for the future of cybersecurity and evaluates the alignment of existing educational and certification programs with industry demands. Employing a mixed-method approach, the study conducts surveys, curriculum analyses, job listings analysis, and literature reviews to provide a holistic understanding of the cybersecurity domain. The findings underscore students' fervent interest in cybersecurity careers despite limited institutional support, emphasizing the need for curriculum refinement and alignment with industry trends. Universities in Kerala should incorporate secure coding, application security, identity and access management in their cybersecurity programs, and consider adding content on cloud security and machine learning to better meet job market demands.

I. INTRODUCTION

Protecting information has emerged as one of the most significant hurdles in the contemporary era. In an age defined by the relentless expansion of the digital realm, cybersecurity stands as an integral bulwark against evolving threats and vulnerabilities. As the world becomes increasingly interconnected and reliant on digital infrastructure, the demand for skilled cybersecurity professionals continues to surge. This study embarks on a comprehensive exploration of the intricate landscape of cybersecurity education and career development, within the context of Kerala, India.

Research Question

What are the essential skills and knowledge areas for various roles within cybersecurity, and how do these requirements vary among roles? Additionally, what emerging skills and areas of expertise are expected to be crucial in the future of cybersecurity, and how do current educational and certification programs in Kerala address the existing skill gaps in the cybersecurity job market?

Research Objectives

- To compile a comprehensive list of essential skills and knowledge areas required for cybersecurity careers.
- To categorize these skills based on different roles within cybersecurity.
- To identify any emerging skills or areas of expertise that are becoming increasingly important in the evolving cybersecurity landscape.
- To investigate students' attitudes towards cybersecurity, their career interests, knowledge, and perceptions.
- To evaluate the effectiveness of existing educational and certification programs in Kerala in bridging the skill gaps that currently exist in the cybersecurity job market.

II. METHODOLOGY

The research methodology for this study employed a mixed-method approach to comprehensively investigate the landscape of cybersecurity skills and education in Kerala. The following methods were utilized**:**

Survey: Conducted a survey among students of the Computer Science Department at Mary Matha Arts and Science College, Wayanad. 26 students participated in the survey Developed a structured questionnaire and was sent to students in google forms. The survey data was analyzed to derive insights into students' attitudes, knowledge, and career interests.

Curriculum Analysis: Collected curriculum and syllabus details from universities and colleges in Kerala providing cybersecurity-related courses. This was done by visiting and checking their institutions website and also by contacting them by phone and mail.

SJIF Impact Factor (2023): 8.574| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 8 | Issue: 10 | October 2023 - Peer Reviewed Journal

Analysis was done to understand the gap between the curriculum and industry requirements, helping predict potential updates in syllabi.

Job Listings Analysis: Analyzed job listing websites such as Naukri, LinkedIn, and Indeed and studied the rate of cybersecurity job postings and the roles and responsibilities associated with various cybersecurity jobs. Also, gathered information about tools and software beneficial for freshers seeking employment in this field.

Review of Published Journals and Research Papers: Searched and selected relevant papers and journals on cybersecurity and identified the futuristic scope of cybersecurity. This helped in understanding emerging skills, technologies, tools, and anticipated changes in the field.

III. ESSENTIAL SKILLS AND KNOWLEDGE AREAS IN CYBERSECURITY

Collecting data on job vacancies from the websites and analysing the pattern, it was found that the following skills and knowledge areas were required for freshers (with 0-to-2-year experience) seeking job opportunities in the field of cybersecurity.

Job Titles	Skills/Knowledges/Tools
Network Security Engineer	**IDS/IPS, Firewalls, Wireshark**
Application Security Specialist **Secure Coding Engineer**	**Application Security (Web / Mobile), Secure Coding Practices, Microservices / API Security, Threat Modelling (STRIDE Or Other)**
Identity Access Management Specialist **Security Policy Developer**	**IAM, Access Management, Security Policy Development, Security Governance Frameworks, Threat Modelling (STRIDE Or Other)**
Security Manager **Cyber Security Consultant** **Security Awareness Trainer**	**Communication Skills, Problem-Solving, Security Policy Development, Security Awareness Training, Change Management, Security Governance Frameworks, Regulatory Compliance**
Information Security Analyst **Security Specialist**	**Security Governance Frameworks, Regulatory Compliance, Risk Management, Security Awareness Training**
Security Engineer **Security Consultant** **Penetration Tester**	**Security Controls, Penetration Testing (Pen Testing), Penetration Testing Tools (Burp Suite, Metasploit, OWASP Zap, OSCP, GPEN, GWAPT), Technical Documentation, Coding**
Cloud Security Engineer	**Cloud Infrastructure Security Requirements, Cloud Security Policies , Secure Cloud Design**
Machine Learning Engineer	**Machine Learning Algorithms, AI Algorithms, Cybersecurity Algorithms, Data Analysis, AI for Threat Detection**

Table 1

IV. The Evolving Landscape of Cybersecurity

From a futuristic perspective, the industry is witnessing a paradigm shift in the skills and areas of expertise required. As cyber threats become more sophisticated, there is a growing demand for professionals well-versed in cybersecurity practices. The ability to predict and proactively defend against cyberattacks using advanced technologies is becoming the new standard.

Ethical hacking techniques are gaining prominence as a proactive approach in identifying vulnerabilities and mitigating risks. Cybersecurity, as a field, now encompasses not only the protection of digital assets but also the assurance of user data privacy and the preservation of an organization's reputation [1]. So, incorporating ethical hacking with cybersecurity benefits for getting employed in companies.

In the current era, there is a surge in the amount of IoT devices used and there is a lot of cyber-attacks on these devices [2]. This vulnerability of intelligent systems makes security a paramount consideration. The ability to secure and protect these technologies from cyber threats is very much significant for a secured future , which emphasizes the importance of learning Internet of Things with cyber security.

In recent times, there has been a surging enthusiasm for harnessing Artificial Intelligence (AI) in diverse cybersecurity contexts. This heightened interest is primarily driven by a growing acknowledgment of AI's importance in combating cyber threats. [3] Hence, the increasing demand for cybersecurity experts with proficiency in AI-driven solutions has surged. The evolving skills and expertise areas within the cybersecurity field include competency in AI and machine learning.

SJIF Impact Factor (2023): 8.574| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 8 | Issue: 10 | October 2023 - Peer Reviewed Journal

Machine Learning plays a crucial role in diverse dimensions of cybersecurity, encompassing functions like identifying phishing attempts, detecting network intrusions, assessing the security of protocols, verifying user identity through keystroke dynamics, ensuring secure communication via cryptography, validating human interactions through CAPTCHAs, and identifying spam content within social networks [4]. Researchers and professionals in this field are exploring various applications of machine learning, such as intrusion detection, traffic classification, and email filtering, to effectively combat cyber threats, including zero-day vulnerabilities [5]. The changing realm of cybersecurity necessitates individuals with knowledge of these machine learning applications to adeptly counter the ever-developing and intricate security threats.

Moreover, as the digital realm continues to expand, the role of cybersecurity is expected to grow exponentially, making it a critical domain for safeguarding our interconnected world.

V. EDUCATIONAL AND CERTIFICATION PROGRAMS IN KERALA

The below mentioned are some of the available Cyber Security courses offered by universities in Kerala.

UG/PG Courses		
University	**Course Offered**	**Skills Taught**
Kerala University of Digital Sciences, Innovation and Technology (Digital University Kerala)	MTech in Computer Science and Engineering with Specialization in Cyber Security Engineering	Security in Digital Transformation Network and System Security Hardware Security Ethical Hacking and Network Defense Advanced Topics in Cryptography
	M.Sc. in Computer Science with Specialization in Cyber Security	Cyber Security and Digital Forensics Modern Cryptography Security Auditing Lab Applied Cryptography Artificial Intelligence for Cyber Security
University Of Kerala	B.Voc Cyber Security	Fundamentals of Information Security Cyber Forensics Network Security Biometrics Security Risk Assessment & Security Audit
Mahatma Gandhi University	B.Sc. Cyber Forensics M.Sc. Cyber Forensic	Internet Technology & Cyber Laws Computer Security Security Threats and Vulnerabilities
APJ Abdul Kalam Technological University	Computer Science and Engineering (Cyber Security)	Cyber Security Essentials Machine Learning Web Application Security Wireless Sensor Network Security Internet of Things

Table 2

As cybersecurity continues to evolve, the need for cloud functionality has increased. SIEM tools have and continue to evolve to function in cloud-hosted and cloud-native environments.

The below mentioned are some of the Cyber Security certification courses available in Kerala.

Certification Courses		
Institution	**Course Name**	**Taught**
ICT Academy of Kerala	Certified Cyber Security Analyst	Foundations of Cybersecurity Network Security and Monitoring Penetration Testing Malware and Metasploit Types of Attacks
Red Team Hacker Academy	Certified Penetration Tester	Networks and Cybersecurity Essentials Security Techniques and Assessments Defense and Protection Social Engineering and Web Security Penetration Testing

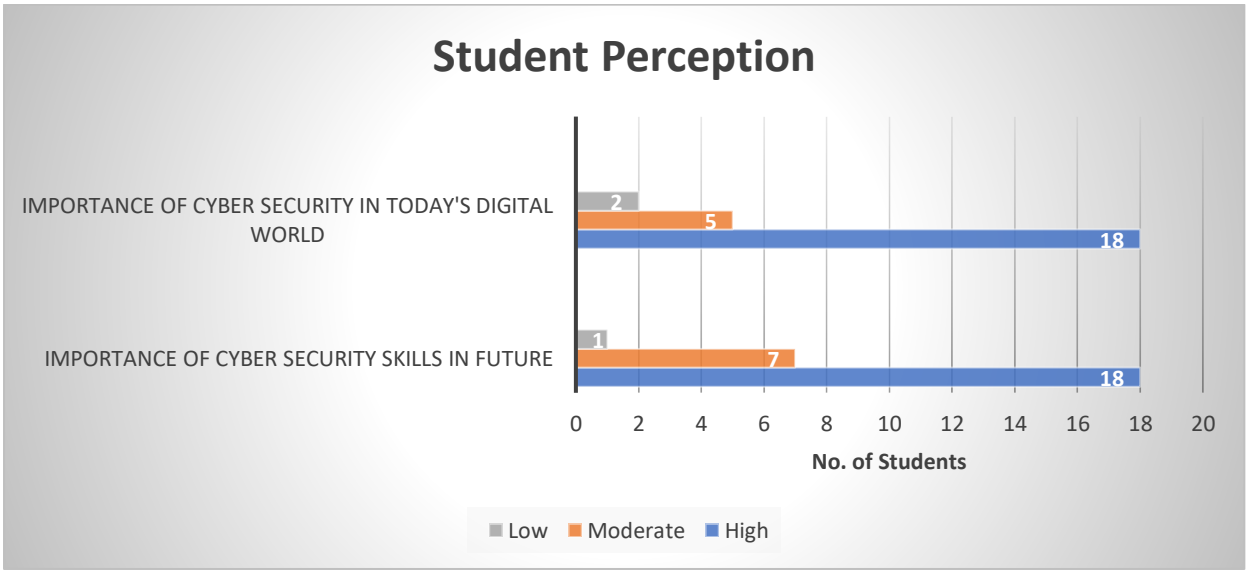
SJIF Impact Factor (2023): 8.574| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 8 | Issue: 10 | October 2023 - Peer Reviewed Journal

	Certified IT Infrastructure Cyber SOC Analyst	Foundations of Cybersecurity Network and System Security Security Information & Event Management (SIEM) Incident Response and Handling Cybersecurity Career Hacking Program
	Ethical Hacker Jr	Introduction to Cybersecurity and Ethical Hacking System Security and Network Communication Hacking and Securing Wireless Networks Bug Bounty Hunting Essentials System Hacking

Table 3

VI. SURVEY FINDINGS: STUDENTS' ATTITUDES TOWARDS CYBERSECURITY

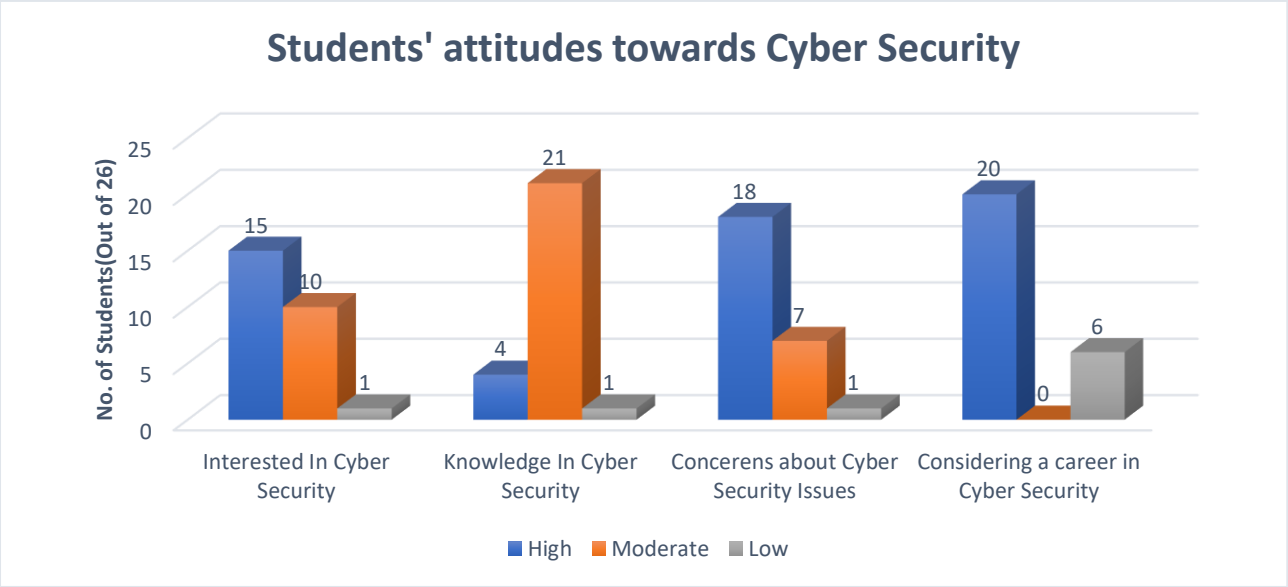
Analysing the survey responses has yielded the following results.:



The above chart describes the perception of students in various aspects of cyber security. 70% of the students who participated in the survey believe that the importance of both cyber security skills in future and cyber security in today's digital world are high. Only less than 7% of students consider cyber security skills unimportant.

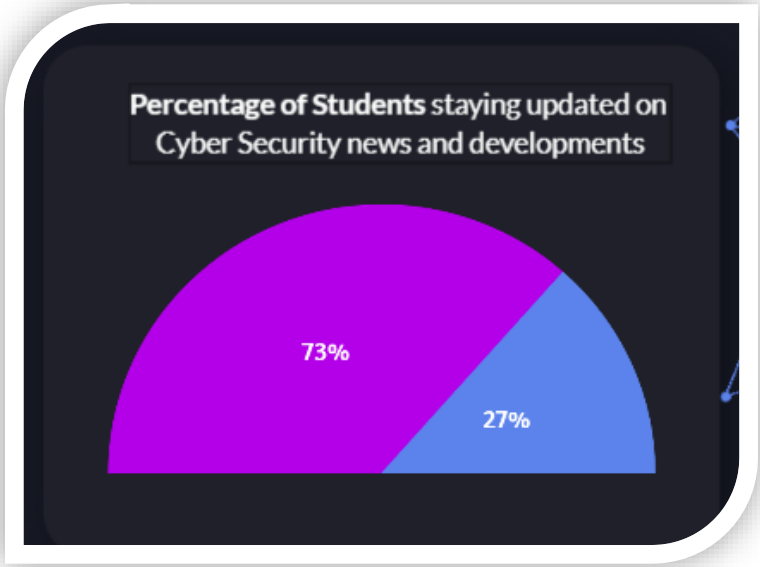
The clustered column below depicts the attitude of students towards cyber security. Their interests, knowledge and concerns are classified into three levels a high, moderate and low. Majority of the students are greatly interested and wish to pursue in this field also they have a moderate knowledge in the area.

SJIF Impact Factor (2023): 8.574| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 8 | Issue: 10 | October 2023 - Peer Reviewed Journal



VII. DISCUSSION & CONCLUSIONS

In the realm of cybersecurity education and career development, the findings of this study underscore the compelling interest and enthusiasm among students for pursuing cybersecurity as a viable career path. It's evident that a substantial number of students are keenly interested in this field and aspire to build careers dedicated to safeguarding digital assets and information. As illustrated in the chart right side 73% of students who participated in the survey are staying updated on cyber security news and developments. However, a significant challenge lies in the current educational landscape, which lacks comprehensive guidance in the foundational aspects of cybersecurity. This gap in the curriculum necessitates a re-evaluation of academic programs to align them with the evolving demands of the cybersecurity job market.



While the courses offered by universities in Kerala cover various aspects of cyber security, there is a need to incorporate more explicit training on secure coding practices, application security, and identity and access management to align with the specific job roles and requirements in the job market. Additionally, considering the importance of cloud security and machine learning in the field, universities may want to consider integrating relevant coursework in these areas. Bridging these skill gaps can help graduates be better prepared for the specific demands of the job market in cybersecurity.

Furthermore, the study highlights the proactive nature of students who exhibit a strong commitment to staying informed about the latest developments in cybersecurity. This self-driven pursuit of knowledge reflects the dynamism and adaptability essential in the cybersecurity domain. It emphasizes the importance of bridging the existing educational gaps to empower aspiring professionals with the requisite skills and expertise. To address these challenges effectively, educational institutions in Kerala should consider refining their cybersecurity curricula, teaching Ethical Hacking lessons, integrating emerging technologies like Artificial Intelligence, Machine Learning, Internet of Things and fostering collaborations with industry experts to provide students with a holistic and up-to-date educational experience. In conclusion, this study calls for a reimagining of cybersecurity education in Kerala, one that aligns with the evolving landscape and equips students with the essential knowledge and skills required to thrive in this ever-changing field.

SJIF Impact Factor (2023): 8.574| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 8 | Issue: 10 | October 2023 - Peer Reviewed Journal

VIII. REFERENCES

1. *Al-Hawamleh, Ahmad & Alorfi, Almuhannad & Al-Gasawneh, Jassim & Al-Rawashdeh, Ghada. (2020), "Cyber Security and Ethical Hacking: The Importance of Protecting User Data'', Solid State Technology, page 5. https://www.researchgate.net/publication/347902323_Cyber_Security_and_Ethical_Hacking_The_Importance_of_Protecting_User_Data.*
2. *S, Naik., V, Maral.,(2017), "Cyber security — IoT", 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), pp. 764-767, https://doi.org/10.1109/RTEICT.2017.8256700.*
3. *Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K. R. ,(2021), "Artificial intelligence in cyber security: research advances, challenges, and opportunities", Artificial Intelligence Review, 55(2), page 2,https://doi.org/10.1007/s10462-021-09976-0.*
4. *Ford, Vitaly & Siraj, Ambareen. (2014). "Applications of Machine Learning in Cyber Security", 27th International Conference o n Computer Applications in Industry and Engineering, CAINE 2014.https://www.researchgate.net/publication/283083699_Applications_of_Machine_Learning_in_Cyber_Security.*
5. *Das, Rishabh & Morris, Thomas. (2017),"Machine Learning and Cyber Security", 2017 International Conference on Computer, Electrical & Communication Engineering (ICCECE),https://doi.org/10.1109/ICCECE.2017.8526232.*