Empowering Cybersecurity Education through HackCyte: A Comprehensive Learning Platform

Nimisha Doshi[1*], Abhijeet Biswas[1], Sameer Shaikh[1], Yash Oswal[1], Aakanksha Kakade[1], Kailas Patil[1*]

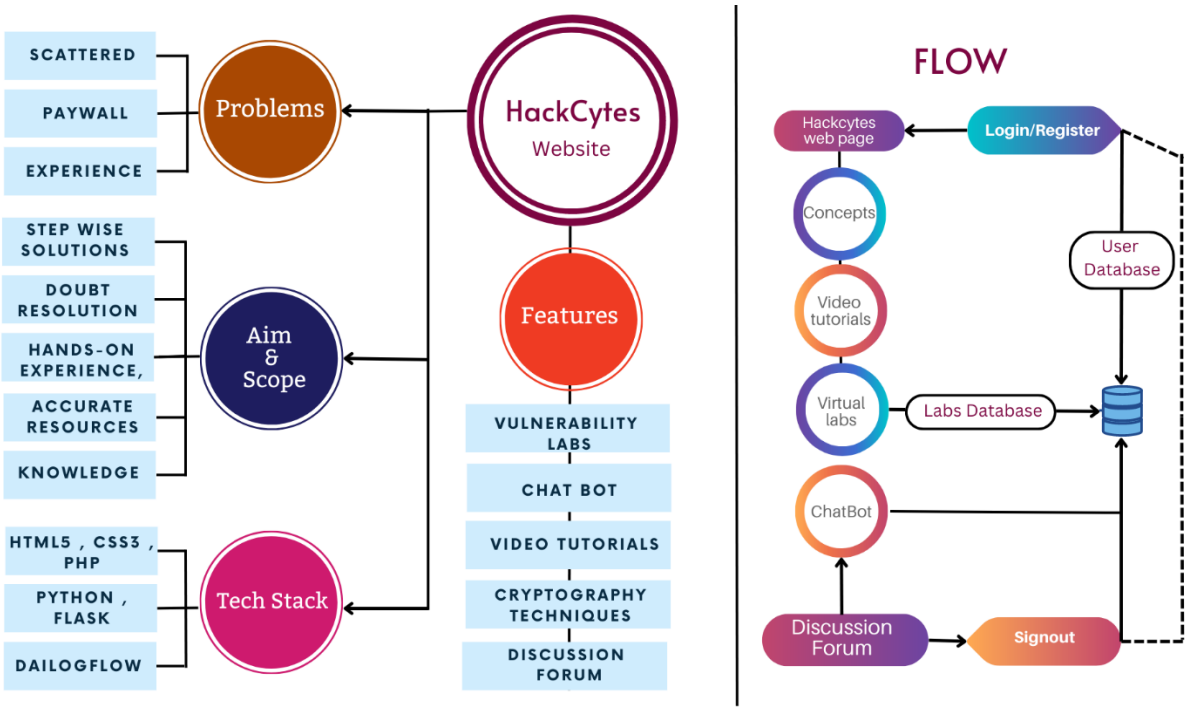
[1] Department of Computer Engineering, Vishwakarma University, 411048,Pune, India

[*] Correspondence: Kailas Patil (kailas.patil@vupune.ac.in); Nimisha Doshi (201900273@vupune.ac.in)

Abstract: This paper presents an overview of existing cyber security methods with the objective of increasing awareness in this critical field. To gather insights, a survey was conducted to assess people's knowledge and opinions on cyber security. The survey findings serve as the foundation for proposing a comprehensive solution to facilitate learning cyber security from scratch. The survey forms were distributed among various educational groups and on diverse social media platforms. The contribution of this paper lies in enhancing learning outcomes and practical skills in the field of cyber security. Through thorough analysis and comprehension within the subject, the drawbacks and regulations of present-day structures were observed. To address these limitations, the identified disadvantages have been reduced, and our proposed remedy takes into account the respondents' feedback. Introducing HackCytes, a comprehensive learning platform, which offers a cutting-edge and engaging approach to cyber security education. The platform incorporates various tools such as peer-to-peer learning forums, interactive chat bots, and vulnerability assessment labs. The ongoing need for qualified professionals to protect against cyber threats and ensure the security of systems and data is emphasized. As the demand for defense against cyber threats continues to grow, there will be numerous opportunities for learning and development in the field of cyber security. Cyber security's significance is expected to increase alongside the widespread use of technology and the internet. With more businesses and individuals relying on technology for various tasks, the likelihood of cyber attacks and other threats will also rise.

Keywords: Cyber security; Chatbot; Teaching; Website; Labs

Graphical Abstract:



1. Introduction

In today's technology-driven world, where network connections and community interactions play a central role in our daily lives, the significance of cyber security cannot be overstated. Safeguarding valuable information, assets, and device data has become a critical defensive measure. Organizations and industries must prioritize cyber security to protect themselves from sophisticated attackers who exploit vulnerabilities in systems using advanced tools and hacking techniques. This is especially crucial considering the sensitive nature of data such as personal information, financial records, and intellectual property stored on various devices and online platforms. Ethical hacking, which involves identifying and addressing vulnerabilities and potential threats, offers an effective approach to securing systems and safeguarding sensitive data.

However, traditional formal education has certain limitations in developing the necessary skills and fostering a network of ethical hackers. To address these limitations, this paper proposes an innovative solution that combines existing cyber security solutions with a comprehensive survey analysis of the challenges faced by individuals aspiring to enter the field of cyber security. The proposed solution takes the form of an educational website designed to make learning about cyber security accessible, interactive, and engaging. This website provides hands-on labs, chat bots, and a discussion forum, empowering individuals to acquire practical knowledge and actively participate in the cyber security community. By bridging the gap between formal education and real-world applications, this website aims to cultivate a strong

network of ethical hackers who can collaborate to enhance overall cyber security.

In addition to its educational role, a cyber security learning website plays a vital role in increasing awareness about the importance of cyber security among individuals, businesses, and organizations. It educates people about the different types of cyber threats and the measures they can take to protect themselves. Moreover, it equips individuals with the necessary skills to defend themselves and their organizations from cyber threats through training on identifying and responding to cyber-attacks and implementing effective security measures. The website also serves as a platform for individuals to acquire the skills and knowledge needed to pursue a career in the cyber security field, which is in high demand. By offering opportunities for employment in the growing field of cyber security, it opens doors for individuals with the necessary skills and knowledge.

Furthermore, a cyber security learning website benefits businesses and organizations by helping them mitigate the risks associated with cyber threats. Through providing employees with necessary training and knowledge, organizations can better protect their networks, data, and other assets from cyber-attacks. By increasing awareness, developing skills, creating career opportunities, and mitigating risks associated with cyber threats, a cyber security learning website plays a significant role in promoting a secure digital environment.

- Section 2: Importance and features of an educational website dedicated to cyber security.
- Section 3: Discussion of the relevant research that informed the study of the cyber security field and compares it with similar existing solutions.
- Section 4: Outline of how our proposed solution overcomes the limitations observed in current models.
- Section 5: In-depth explanation of the survey objectives, scope, methodology, and data collection process.
- Section 6: To offer a comprehensive understanding of the website's architecture, this section presents a clear overview of its components, features, and functionality.
- Section 7: Potential future project ideas.
- Section 8: Concludes the paper, summarizing the key findings and highlighting the significance of the proposed website as a crucial step toward strengthening cyber security.

2. Literature Review

Different papers have been studied summarised. Method / Model / Algorithm used Important Features, Accuracy / Conclusion / Result, Disadvantages /Advantages are represented in form of table. Research papers from cyber security domain have been thoroughly analysed and their advantages, disadvantages and limitations have been studied.

Table 1 Shows the Method / Model / Algorithm used, Important Features, Accuracy / Conclusion / Result, Disadvantages /Advantages of the research papers that involve cyber security awareness.

Sr. No.	Method / Model / Algorithm used	Important Features	Accuracy / Conclusion / Result	Disadvantages /Advantages	Ref
1	University Students researched in Siberia, particularly freshmen.	Study cyber security awareness and determine the effects of variables like socio-demographics, cyber security perceptions, past cyber security breaches, IT usage, and knowledge to cyber security behavior.	impact of perceptions of cyber security effectiveness. When compared to effects, knowledge, experiences, and are stronger. Sociodemographic for cell phone-related behavior, or in particular, IT usage and information, became important cellular behavior indicators.	There haven't been any useful predictors discovered for password behavior.	Kovačević et al. (2020)
2	The framework is based on the novel idea of the stochastic cyber attack process, a new class of mathematical objects for describing cyberattacks.	1) Statistical framework for objectively evaluating and utilizing information from cyberattacks detected by honeypots. 2) To analyze data, the framework employs a honeypot with minimal interaction. 3) The framework is used to analyze honeypot data with low and high interaction; it provides insightful information on attacks and enables finer-resolution analysis.).	The framework describes attacks against production networks.	Datasets used in research are insufficient and attack-neutral, respectively. Instead of the production network, a honeypot is used to collect the data.	Zhan et al. (2013)

3	The discussion includes recommendations for better attribution and future research directions as well as the current state of attribution capabilities for both types of attacks.	The discussion of attribution in this paper is focused on network intrusions and social bot-led misinformation campaigns, these attacks that are fundamental to contemporary cyberspace conflict.	The study's main emphasis is on digital forensics using network intrusions and social bots that disseminate false information.	The study falls short in that it only covers network intrusions and social bot-led misinformation, which is insufficient to provide comprehensive knowledge about cyber security.	Goel and Nussbaum (2021)
4	The issue of automated HTTP (Hypertext Transfer Protocol) request structure analysis applied to web layer cyberattack detection is addressed in this article.	Combining the machine-learnt classifier with the clustering algorithm for HTTP sequences. It is not necessary to have prior knowledge of the HTTP-based APIs and protocols.	The new technique for detecting HTTP Traffic Anomalies has been proposed by researchers in this article. The derived method gives potential effective performance and outcomes by using knowledge of the HTTP payload structure.	The method proposed in the paper does not use weekly data to analyse the HTTP payloads.	Kozik et al. (2017)
5	Decoy-based deception model, decoys, deception, and artificial intelligence, RNN model	1) Confuses eavesdroppers' time and resources by encrypting the message into an unreadable format. 2) An instant messaging program that incorporates cutting-edge encryption techniques.	1) In the terms of English texts, natural language decoys are used to reduce the threat of eavesdropping. 2) While the message is being hidden from the plaintext, a dummy message is generated based on the category of the plaintext.	Does not cover all the encryption schemes which could be better to prevent brute force attacks	Omolara et al. (2019)

6	1)formally published literature; journal and conference workshop 2) grey literature, white papers, website, reports along with blogs	1)Types of social engineering attacks, approach definitions and goals 2) Motivation behind the attacks 3) limitations	1) Surveys reveal that 96% of respondents use machine learning and artificial intelligence (AI) tools for cybersecurity. 2) detects a state of creativity. and practice current social engineering techniques, attacks, and platforms used for cyber-attacks/threats	Does not provide in detail study about those attacks and how they can occur	Hijji and Alam (2021)
7	An analysis of XSS vulnerability exploitation and detection techniques.	there are three types of analysis: hybrid, dynamic, and static.	XSS classification, first. 2) A demonstration website for attacks using common XSS. Prevention strategies.	1) The recall rate and precision rates for static analysis are 85.1 percent and 84.9%, respectively. 2) Precision rates for dynamic analysis are 97.2 percent and 0 percent, respectively, for false positives. The method has a false-positive rate of 9% when predicting XSS vulnerabilities, which is a bit high.	Liu et al. (2019)
8	Security of SMBs, NIST Cyber Security Framework (CSF),	1)SMB face Challenge in options of implementing good cyber security 2)Approaches include powerful quantitative research	1) Nations don't take SMB cybersecurity into account. 2) The areas of practical implementation, detection, response, and its recovery are underdeveloped.	1) Some categories from the Detect, Respond, and Recover functions were not represented at all, while other categories were not represented at all. 2) Little research has been done on cyber resilience.	Chidukwani et al. (2022)

9	Methodology includes defining and analyzing various strategies attackers use.	Deter: Preventing the attacker from accessing information during recon. Detection: Monitoring system to quickly detect the likelihood of an attack. Defend: Having a well-laid out disaster recovery plan.	This paper goes over strategies of attackers and quick counter action to them through deterring, detecting and defending.	This paper goes over vaguely how employee negligence can be escalated to highly orchestrated attacks.	On uo ha (20 18)
10	a plan for the integration of cybersecurity into the curriculum.	to educate K–12 students, college students, technical professionals, and all other citizens. numerous remedies for issues relating to cybersecurity.	1) Their cybersecurity skills would give them a significant advantage in the job market. 2) The development of cyber security is dependent upon education.	Does not place a greater emphasis on leadership or technical programs related to cyber security.	Ah ma d et al. (20 22)
11	1) The front-end behavioral level; 2) the middle Register Transfer Level (RTL); and 3) the back end gate-level simulation-based defect analysis.	overcoming the difficulties of advanced education internationally.	1)Universities should integrate international schemes of collaboration and networking 2) Efforts are taken to promote interest such schemes	Proper knowledge to provide to cyber professional or students in order to study in depth about cyber physical systems	Vie rha us et al. (20 14)
12	Modular approach	1)Standalone modules integrated with various technical courses 2) cyber secure programming concepts	Cyber security learning concept modules as a complete independent package and incorporate in a course	Derived various new concepts of integrating labs and modules with solutions and developing cyber security concepts	Lod gh er et al. (20 18)
13	1)Hour workshop model 2)surveys 3)week-long intervention	1) Compared to men, women are better at solving problems and growing as independent cybersecurity professionals.	The desired positive outcome is produced by the intervention's necessary intensity and type.	One-time, short-term models might not be enough to produce significant results.	Am o et al. (20 19)

14	Research into the security and privacy issues caused by the interaction between the physical and digital worlds.	(1) Analyzing fresh attack types and constructing an attack model based on prior research. 2) Better defenses against the new physical and cybernetic threats.	1) Convert outdated literary defenses into distinct attack vectors. 2) abstract conditions for defenses against cyber-physical attacks.	Attacks that use information leakage and signal injection to compromise physical domains are known as cyber-physical attacks.	Yu et al. (2021)
15	Review of the honeypot and honeynet research in the IoT, IIoT, and CPS.	1) A thorough analysis of earlier honeypots and honeynets identifies important design elements. 2) Additional issues and research on honeypots and honeynets.	1) Determined the fundamental characteristics of honeypots and honeynets for IoT, IIoT, and CPS. 2) Attempts to incorporate honeypots and honeynets with IDS software.	extensive details about honeypots and honeynets, along with important considerations.	Franco et al. (2021)
16	Cyber resilience maturity of a particular sector can be evaluated against an established collection of markers which will act as an expression set for establishing cyber-resilience.	Methodology used: 1.Assessment of current sector design and operation. 2.Evaluating against expressions set will give a rating based on assessment of the sector's cyber resilience.	Exploring Cyber Resilience across sectors is one of the important features of Progress. Another important feature is to build holistic progression levels to advance in maturity phases of a sector.	Some maturity models can be ill-suited to a sector and thus, lead to inefficient spending over resources that could have been dealt with alternatively.	Shaked et al. (2021)
17	Implementation of Fail- proof system via MYSQL Replication technique based on three tier layers.	Three tiers: 1.First tier shows a telecom provider as an ISP. 2. ISP for a tier 2 organisation like Bank. 3. Tackling attacks like DDos without disruption in service.	Implementation of a fail-proof system for a cyber security environment with novel approach in deploying these systems.	The fail-proof system can fail itself so that is an important element that needs to be considered as well.	Isiaka, Audu, and Umar (2020)

18	Understanding the business and the data, preparing the data, modeling, evaluating the results, and deploying the solution are the six phases of the CRISP DM approach. The training and testing phases of the ML approach.	1. Analysis of methods applied to intrusion detection systems. 2. Analysis of different data sets. 3.Application of DM and ML data sets to cyber.	This paper goes over the ML and DM method applied to cyber intrusion detection systems. Generating and sampling sets can be an arduous task, but it can be worth it if it is sampled and labelled, it can be fruitful to use them as the intrusion methods are incredibly complex.	The disadvantage of this is that even if it is good at detecting behaviour through trained data sets, for situations that are abnormal, it can generate a large number of false alarms. Also, the models need to keep up with developments and recent updates to predict behaviour correctly.	Buczak and Guven (2016)
19	A hybrid scheme is suggested in this paper which increases system soft error reliability, including running simulated experiments to justify efficiency of the given hybrid scheme.	Related features in this are Application and Hardware model, soft-error and lifetime reliability model, security service model.	This paper is about overcoming the constraints faced during workflow scheduling problems during CPCS.	Scheduling discipline used may not suit the framework of an organisation, it is necessary for a well-informed individual to choose it.	Zhou et al. (2021)
20	This paper first reviews the different types of cyber-crimes and various strategies that can be used to overcome it.	Features include cybercrime types, cybercrime detection techniques and other methodologies.	This research paper analyses the different types of cybercrimes and studies along with the various datasets and challenges faced to avail benchmark datasets.	This paper has a downside where the different detection techniques in place may act aberrant or not work as intended.	Al-Khater et al. (2020)

A. Kovačević, N. Putnik and O. Tošković, "Factors Related to Cyber Security Behavior",The article "Factors Related to Cyber Security Behavior" explores the factors that influence individuals' cybersecurity behavior based on a survey of 1,069 respondents in Serbia. The study found that perceived risk, knowledge and awareness of cybersecurity, self-efficacy, and perceived control were important factors that influenced cybersecurity behavior. The results also showed that age, education level, and gender were significant factors in determining cybersecurity behavior. The study emphasizes the importance of understanding these factors in

developing effective cybersecurity awareness programs.

Z. Zhan, M. Xu and S. Xu, "Characterizing Honeypot-Captured Cyber Attacks: Statistical Framework and Case Study", the article presents presents a statistical framework for characterizing cyber-attacks using data captured from honeypots. It also provides insights into the nature of cyber-attacks and demonstrates the potential of using honeypots as a tool for improving network security. We use this framework to build virtual labs for users to demonstrate cyber-attacks.

S. Goel and B. Nussbaum, "Attribution Across Cyber Attack Types: Network Intrusions and Information Operations,"The authors highlight the differences between these two types of attacks and examine the challenges of identifying their perpetrators. The study also discusses the various techniques used in attribution, including technical, behavioral, and geopolitical methods. This attribute helps to overcome challenges in cyber attack.

M. Liu, B. Zhang, W. Chen and X. Zhang, "A Survey of Exploitation and Detection Methods of XSS Vulnerabilities,"The authors present a survey of the latest research on XSS vulnerabilities, covering various types of attacks, such as stored, reflected, and DOM-based XSS, and discussing different approaches to detecting and mitigating these attacks. The study also provides an in-depth analysis of various tools and techniques used to exploit and detect XSS vulnerabilities. Overall, the article offers a valuable resource for researchers and practitioners interested in improving their understanding of XSS vulnerabilities and developing effective mitigation strategies.

N. Ahmad, P. A. Laplante, J. F. DeFranco and M. Kassab, "A Cybersecurity Educated Community,"The authors argue that cybersecurity education is essential to mitigating the growing threat of cyber attacks and propose a three-pronged approach to building a cybersecurity-educated community. The approach involves promoting cybersecurity awareness, providing cybersecurity education, and establishing cybersecurity partnerships between industry, academia, and government. The study also discusses various challenges and opportunities associated with implementing this framework and provides recommendations for future research in the field of cybersecurity education. Overall, the article highlights the importance of cybersecurity education in building a secure and resilient digital society.

D. Onuoha, "Cyber Defense: Deter, Detect, and Defend,"The author emphasizes the importance of taking a proactive approach to cyber defense and highlights the need for organizations to establish clear policies and procedures for responding to cyber-attacks. The study also discusses various tools and techniques that can be used to detect and mitigate cyber threats, including intrusion detection systems, firewalls, and security information and event management (SIEM) solutions. Overall, it emphasizes the importance of ongoing training and education to ensure that organizations are equipped to respond effectively to the ever-evolving threat of cyber-attacks.

A. Lodgher, J. Yang and U. Bulut, "An Innovative Modular Approach of Teaching Cyber Security

across Computing Curricula,"The authors argue that cybersecurity should be integrated into all computing courses, rather than being taught as a standalone subject, and propose a modular approach that can be customized for different computing courses. The study describes the development of a set of modular cybersecurity units that can be integrated into existing courses, such as software engineering, database systems, and networking. The authors also discuss various tools and techniques that can be used to teach cybersecurity, such as simulations, case studies, and hands-on exercises. The article concludes by highlighting the importance of this approach in preparing computing students for the challenges of a rapidly evolving cybersecurity landscape.

Z. Yu, Z. Kaplan, Q. Yan and N. Zhang, "Security and Privacy in the Emerging Cyber-Physical World: A Survey,"The authors provide a detailed analysis of the different types of cyber-physical attacks, including physical attacks, software attacks, and network attacks. The article also discusses various defense mechanisms that can be employed to mitigate these attacks, such as authentication, access control, intrusion detection, and privacy protection. The study concludes by highlighting the importance of developing secure and resilient cyber-physical systems to ensure their safe and reliable operation in the face of evolving security threats.

4. Overcoming Limitations

The proposed cyber security solution considers the drawbacks and limitations of existing systems and leads to significant improvements. It focuses on improving cyber security skills through a combination of interactive exercises and theoretical content. These exercises cover the basics of cyber security, including encryption methods and teach participants preventive measures to combat various cyber attacks.

In addition, our solution makes cyber security education accessible to the public. We provide educational content that helps raise awareness and understanding of cyber security among a wider audience. Further, we keep abreast of the latest developments and events in cyber security to ensure that the knowledge imparted is current and relevant.

To facilitate effective learning and problem solving, our solution includes clear definitions, query and remediation capabilities, and vulnerability assessment and remediation information. By providing individuals with the necessary tools and resources, we empower them to protect themselves and their systems from cyber threats.

Therefore, more descriptive methods to improve cyber protection skills were carried out structurally, and students should learn how to protect themselves from cyber attacks not only in theory but also in the laboratory. Onuoha (2018) emphasized teaching vulnerability skills and protection against them in the form of labs so that employees can learn how to protect themselves. Integrating digital labs so that people can engage in an interactive environment to gain more knowledge and answers Ideas from Hijji and Alam (2021), Amo et al. (2019) Mitigation

is achieved by designing labs for different vulnerabilities so that consumers know how exactly a vulnerability can be exploited and how to avoid it in a system. Liu et al. (2019) advise classifying XSS vulnerabilities similarly and designing demo labs for such attacks so that users can enjoy running such attacks. Kovačević et al. (2020) report that while there are extensive sources on the Internet as well as some tutorials, they have not proven to be powerful learning tools for students anymore. Therefore, more descriptive methods of improving cyber protection knowledge were carried out to teach students how to protect themselves from cyber attacks not only in theory but also in exercises. Onuoha (2018) focused on providing expertise on vulnerabilities and how to protect against them by conducting exercises to help employees learn how to protect themselves. Integrating digital labs to create an interactive environment for more knowledge and answers is a facilitator for Lodgher et al. (2018).

The basics of cyber security are covered by our web application-based system as learned from Goel and Nussbaum (2021). All encryption schemes have been included in the content so that the user knows which algorithm to apply in the future, to mitigate the limitations of Ahmad et al. (2022), detailed and guided preventive measures for various cyber security attacks and instructions for implementation are provided. Educational content will be provided for the masses to learn about various systems, their uses, and how they work according to Vierhaus et al. (2014). Different concepts of cyber attacks are included and further classification of attacks by their domain is done to reduce the shortcomings in Yu et al. (2021). In Shaked et al. (2021), it is emphasized that individuals need to be aware of the latest developments in cyber security in order to choose the right resilience model. The latest knowledge about cyber security events has been made available, which serves as a reservoir of information so that an employee is better able to select the right maturity model with the desired information in mind. The solution for Zhou et al. (2021) is to provide information about cyber security and various vulnerabilities that keep users informed about the latest updates on a particular topic. To mitigate the limitations of Al-Khater et al. (2020), our platform provides information about vulnerability analysis and how to deal with it; a person who has access to it can perform a manual analysis when automation fails. In this way, we try to mitigate the drawbacks and limitations of existing systems in the proposed solution.

In summary, our proposed solution aims to overcome the limitations of existing systems by providing a comprehensive and effective approach to cyber security. It combines interactive learning, hands-on exercises, educational content, and up-to-date knowledge to increase cyber security awareness and skills.

5. Survey Analysis

5.1 Survey Objective

The purpose of the survey was to gather information about users' interests and preferences so that the website could incorporate these features and enhance user experience as a result.

5.2 Survey Design

A survey was designed and conducted to gain insight into people's knowledge and opinions about cyber security. The goal of the survey was to determine the current level of knowledge and gather feedback that served as the basis for proposing a comprehensive solution to facilitate learning cyber security from the ground up. Survey forms were distributed to various educational groups and through various social media platforms to ensure that a wide range of participants and perspectives were included in the data collection process.

5.3 Participant Demographics

A survey was conducted to gauge the interest and requirements of students from various streams, including Computer Engineering, Electronics, Mechanical, Electrical, IT, Civil, Artificial Intelligence and Data Science, Pharmacy, and professionals, in the field of cyber security. The survey revealed that 68.6% of the total participants were interested in learning and exploring the cyber security domain, and this interest was reflected across all specializations. Even among Artificial Intelligence and Data Science students, 71.4% expressed an interest in learning cyber security.

5.4 Key Findings

The survey participants expressed a preference for a website with an interactive chatbot, video tutorials, and labs over traditional teaching methods like books and offline learning. Participants also expressed a strong interest in securing websites and participating in bug bounty programs. Ethical Hacking emerged as the most dominant topic of interest for survey participants, followed by Application security and data security. Other domains of interest included network security, penetration testing, and cryptography.

The survey also highlighted the challenges faced by learners, including lack of guidance, expensive learning materials, scattered resources, and a lack of cyber security topics in their coursework. Suggestions provided by survey participants to include a discussion forum to resolve doubts. Overall, the survey was designed with careful consideration of user requirements, challenges, and interests that ensured the inclusion of participants from various backgrounds.

5.4 Incorporating Survey Results into the Website.

These specifications were taken into consideration when creating the website, which offers a variety of labs and resources for students to use. The top 10 OWSAP vulnerabilities were taken into account during the design of the labs. The website was developed to offer information and labs relevant to all these themes because hands-on labs were the most often requested user requirement in the survey. When creating the website, which aspired to provide a comprehensive learning platform for all interested students, the challenges were taken into mind. Overall, user requirements, difficulties, and interests were carefully considered when

establishing and designing the website, according to the survey of participants from varied backgrounds.

6. Proposed System

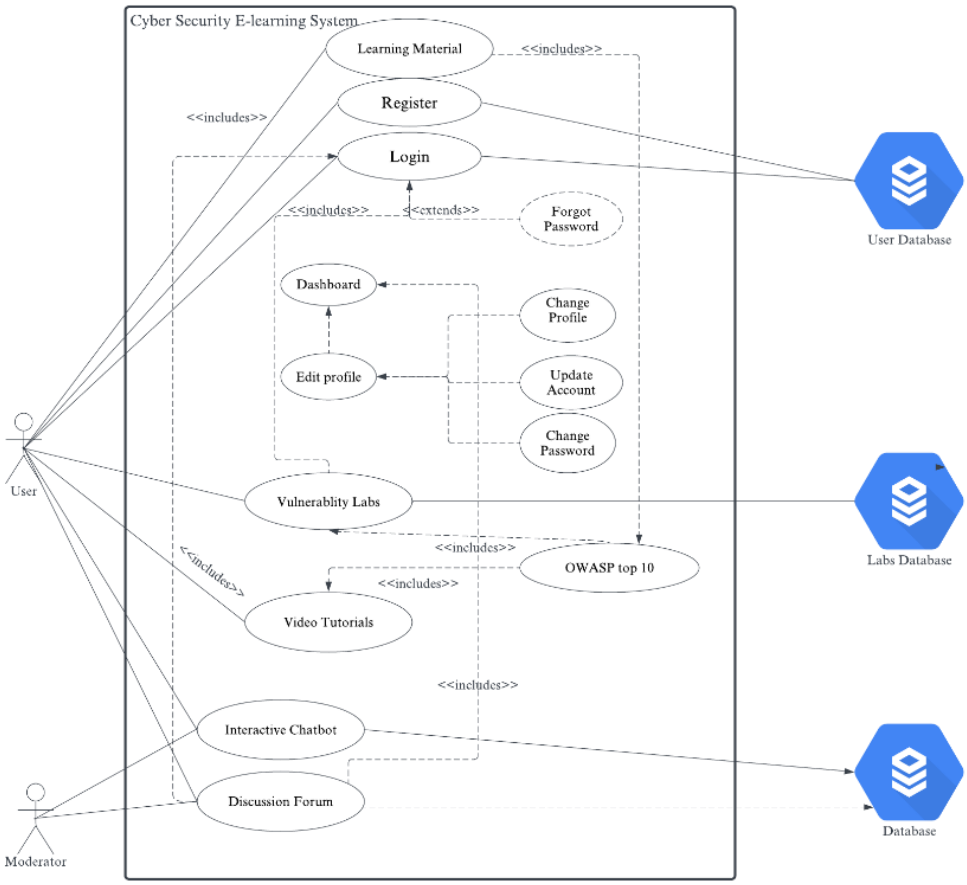


Figure 1. Use case diagram for overall system is pictorially represented.

HackCytes is a recently developed and launched website which features beginners and individuals looking to hone their cyber security skills and anybody who is interested in cyber security can learn, apply and test their skills. This project has been materialized in the form of a website wherein we include learning material, labs, a discussion forum and a chatbot to aid users with queries. Accurate resources that are required to start learning from beginner to advance level stepwise are added. Free-of-cost resources/materials on cyber security are present so that everyone can learn and protect themselves from cyber threats. Figure 1. Shows use case diagram of the proposed solution.

6.1 Website

For absolute beginners and people looking to develop their knowledge of cyber security, the latest information covering different domains of cyber security has been included. As seen in Figure 2. The topics that are covered in HackCytes are an introduction, cryptography, application security, data security, ethical hacking, and network security.

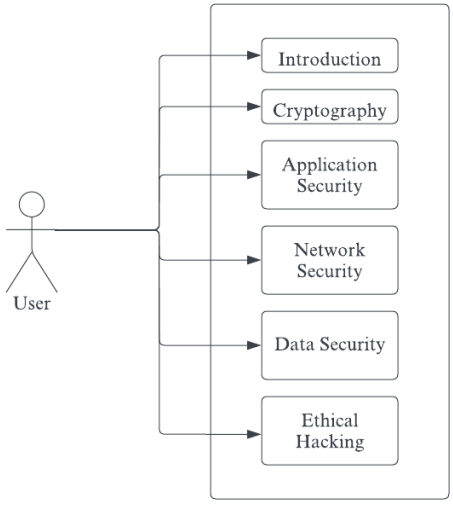


Figure 2. Use case diagram for website is pictorially represented.

6.2 Chatbot

The chatbot has been implemented using Dialogflow. A conversational user interface can be easily designed and integrated into your mobile app, web application, device, bot, interactive voice response system, etc. using Dialogflow, a platform for natural language understanding. By utilizing Dialogflow, users are offered fresh and interesting ways to engage with the system. Chatbot has been defined with capabilities and interactions best suited for beginner interaction. Users can search for the most asked questions, doubts and other such queries. Over time chatbot can recognize patterns in language and adapt accordingly. Figure 3 shows a use case diagram for how chatbot will be designed and integrated.

The user's interaction with the chatbot can be significantly influenced by how well the bot copy performs. Poorly written bot copy can make the chatbot seem robotic or be challenging to understand, while well-written bot copy can make the chatbot feel more natural and engaging to the user. Botcopy has been integrated to enhance the capabilities of Dialogflow by adding menu, suggestion chips, audio input-output, color and Avtar of the bot.

Janis.ai is designed to be easy to use, with a visual interface and pre-built templates and components that allow users to create chatbots without needing to have programming skills. Janis.ai offers a range of options for building and customizing chatbots, including the ability to use the platform's API to build custom integrations and features. Janis has been integrated so that the user can directly interact with the experts.

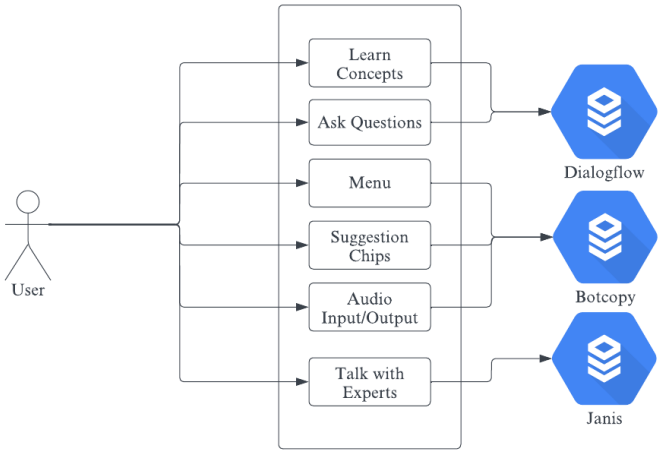


Figure 3. Use case diagram for Chatbot is pictorially represented.

6.3 Labs

Labs included in our system are designed to be vulnerable to a variety of common web application vulnerabilities. It can be used as a training tool for individuals who want to learn about web application security and how to identify and exploit vulnerabilities.

Websites include a variety of realistic vulnerabilities that are commonly found in web applications, including HTML injection, SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). Educational: Website includes detailed explanations of each vulnerability, along with examples of how they can be exploited.

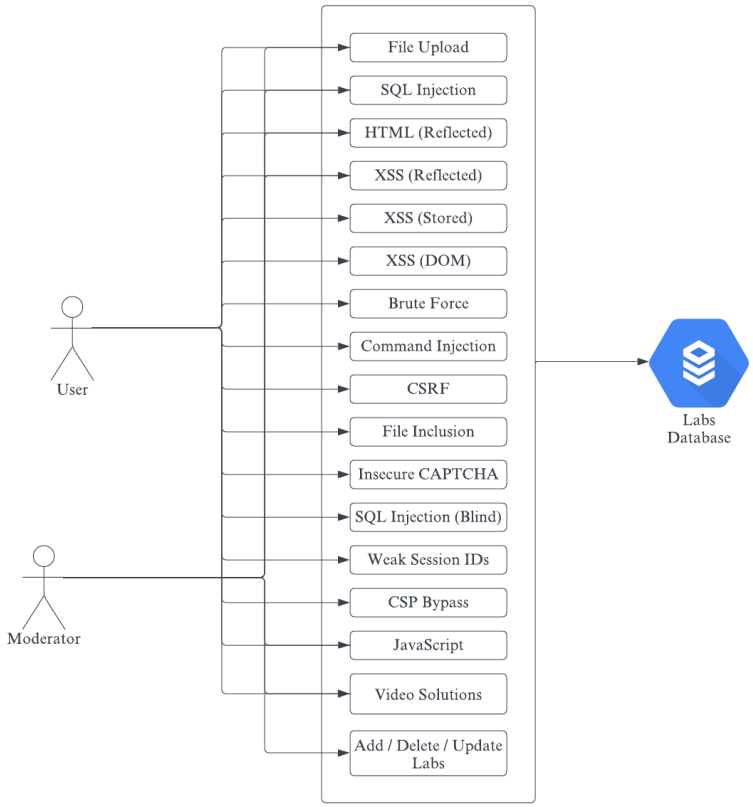


Figure 4. Use case diagram for labs is pictorially represented.

6.4 Discussion Forum

Users can create new threads or topics for discussion and post their doubts. Users can reply to existing threads or topics and contribute to the discussion. Forum classifies the doubts into categories so that the user can find threads or topics that are relevant to their interests. Users have their own profiles where they can share information about themselves and their interests.

The forum has a moderator who can enforce rules and ensure that discussions are respectful and appropriate. The forum has a notification system that alerts users when there are new replies to threads that they are participating in or following. The forum is accessible from mobile devices, as many people use their phones and tablets to access the internet. Figure 5. Depicts use case diagram of discussion forum showing various functionalities that it can provide.

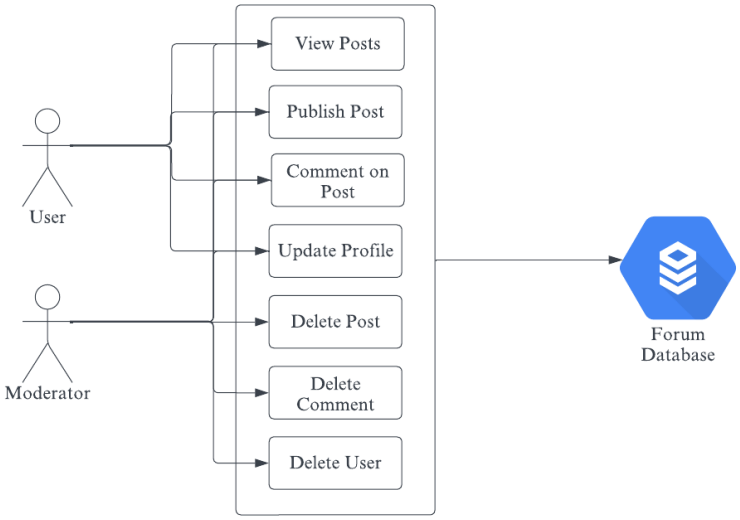


Figure 5. Use case diagram for discussion forum is pictorially represented.

7. Future Scope

The field of cybersecurity is constantly evolving, and there is always a need for skilled professionals who can help to protect against cyber threats and ensure the security of systems and data. There will be many opportunities for learning and growth in the field of cybersecurity in the future, as the need to protect against cyber threats continues to grow. Proficiency in these areas will be important for those interested in pursuing a career in cybersecurity, as well as for organisations looking to hire cybersecurity professionals. As technology and the internet become more prevalent, the need for cybersecurity is expected to grow. As more organisations and individuals rely on technology and the internet for various tasks, the risk of cyber-attacks and other threats will also increase.

Continuously updating and expand educational content on the website to cover emerging cyber security threats, new attack techniques, and evolving technologies. This may include providing detailed guides, tutorials, case studies, and real-world examples to keep users up-to-date on the latest trends in cyber security. Introduce more interactive learning tools and simulations to create a hands-on learning experience for users. Build a strong community around the website by incorporating features such as discussion forums, online chat groups, and collaboration platforms.

To enhance user engagement and encourage skill development, the website can include gamification elements such as earning badges, completing challenges, and participating in contests. This interactive approach adds enjoyment and motivation to the learning process. Through partnerships with recognized certification bodies or organizations, the site can also offer accredited cyber security courses or certification programs. This not only increases the credibility and value of the educational content but also allows individuals to showcase its own expertise in the field.

Regularly collect user feedback and conduct surveys to identify areas for improvement and refine site features and content. This iterative approach allows the site to adapt to evolving

user needs and preferences and remain relevant in the dynamic field of cyber security.

8. Conclusions

In conclusion, the significance of cyber security in our everyday lives can't be overstated. With a lot of our private and economic data being saved online, its miles important to defend ourselves in opposition to cyber-assaults and hold believe within side the safety of our online systems. As the era keeps advancing, the call forprofessional cyber security experts is on the rise, and its miles critical to make certain that right training and education are to be had to satisfy this call for.

Our proposed system, HackCytes, is a complete mastering platform that gives a modern and interactive method to cyber security training. With capabilities like vulnerability evaluation labs, an interactive Chabot, and a dialogue discussion board for peer mastering, HackCytes makes mastering approximately cyber security accessible, engaging, and fun.

By the usage of this platform, absolutely everyone can study cyber security from scratch and take advantage of the abilities and know-how had to defend themselves and others online. Overall, the improvement and use of structures like HackCytes are vital for advancing cyber security training and education, and for growing a network of professional cyber security experts who can correctly deal with the ever-evolving threats of the virtual age.

References

A. Chidukwani, S. Zander and P. Koutsakis, "A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations," in IEEE Access, vol. 10, pp. 85701-85719, 2022, doi: 10.1109/ACCESS.2022.3197899.
Parenthetical citation: (Chidukwani et al., 2022)
Narrative citation: Chidukwani et al. (2022)

A. Kovačević, N. Putnik and O. Tošković, "Factors Related to Cyber Security Behavior," in IEEE Access, vol. 8, pp. 125140-125148, 2020, doi: 10.1109/ACCESS.2020.3007867.
Parenthetical citation: (Kovačević et al., 2020)
Narrative citation: Kovačević et al. (2020)

A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," in IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153-1176, Secondquarter 2016, doi: 10.1109/COMST.2015.2494502.
Parenthetical citation: (Buczak&Guven, 2016)
Narrative citation: Buczak and Guven (2016)

A. Lodgher, J. Yang and U. Bulut, "An Innovative Modular Approach of Teaching Cyber Security across Computing Curricula," 2018 IEEE Frontiers in Education Conference (FIE), 2018, pp. 1-5, doi: 10.1109/FIE.2018.8659040.
Parenthetical citation: (Lodgher et al., 2018)
Narrative citation: Lodgher et al. (2018)

A. Shaked, L. Tabansky and Y. Reich, "Incorporating Systems Thinking Into a Cyber Resilience Maturity Model," in IEEE Engineering Management Review, vol. 49, no. 2, pp. 110-115, 1 Secondquarter,june 2021, doi: 10.1109/EMR.2020.3046533.
Parenthetical citation: (Shaked et al., 2021)

Narrative citation: Shaked et al. (2021)

D. Onuoha, "Cyber Defense: Deter, Detect, and Defend," in SMPTE Motion Imaging Journal, vol. 127, no. 6, pp. 1-6, July 2018, doi: 10.5594/JMI.2018.2832003.
Parenthetical citation: (Onuoha, 2018)
Narrative citation: Onuoha (2018)

E. Omolara, A. Jantan, O. Isaac Abiodun, K. Victoria Dada, H. Arshad and E. Emmanuel, "A Deception Model Robust to Eavesdropping Over Communication for Social Network Systems," in IEEE Access, vol. 7, pp. 100881-100898, 2019, doi: 10.1109/ACCESS.2019.2928359.
Parenthetical citation: (Omolara et al., 2019)
Narrative citation: Omolara et al. (2019)

F. M. Isiaka, S. A. Audu and M. A. Umar, "Developing a fail-safe culture in a cyber environment using MySQL replication technique," in International Journal of Crowd Science, vol. 4, no. 2, pp. 149-170, June 2020, doi: 10.1108/IJCS-04-2018-0008.
Parenthetical citation: (Isiaka, Audu, & Umar, 2020)
Narrative citation: Isiaka, Audu, and Umar (2020)

H. T. Vierhaus, M. Schölzel, J. Raik and R. Ubar, "Advanced technical education in the age of cyber physical systems," 10th European Workshop on Microelectronics Education (EWME), 2014, pp. 193-198, doi: 10.1109/EWME.2014.6877424.
Parenthetical citation: (Vierhaus et al., 2014)
Narrative citation: Vierhaus et al. (2014)

J. Franco, A. Aris, B. Canberk and A. S. Uluagac, "A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems," in IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2351-2383, Fourthquarter 2021, doi: 10.1109/COMST.2021.3106669.
Parenthetical citation: (Franco et al., 2021)
Narrative citation: Franco et al. (2021)

J. Zhou, J. Sun, M. Zhang and Y. Ma, "Dependable Scheduling for Real-Time Workflows on Cyber–Physical Cloud Systems," in IEEE Transactions on Industrial Informatics, vol. 17, no. 11, pp. 7820-7829, Nov. 2021, doi: 10.1109/TII.2020.3011506.
Parenthetical citation: (Zhou et al., 2021)
Narrative citation: Zhou et al. (2021)

L. C. Amo, R. Liao, E. Frank, H. R. Rao and S. Upadhyaya, "Cybersecurity Interventions for Teens: Two Time-Based Approaches," in IEEE Transactions on Education, vol. 62, no. 2, pp. 134-140, May 2019, doi: 10.1109/TE.2018.2877182.
Parenthetical citation: (Amo et al., 2019)
Narrative citation: Amo et al. (2019)

M. Hijji and G. Alam, "A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions," in IEEE Access, vol. 9, pp. 7152-7169, 2021, doi: 10.1109/ACCESS.2020.3048839.
Parenthetical citation: (Hijji&Alam, 2021)
Narrative citation: Hijji and Alam (2021)

M. Liu, B. Zhang, W. Chen and X. Zhang, "A Survey of Exploitation and Detection Methods of XSS Vulnerabilities," in IEEE Access, vol. 7, pp. 182004-182016, 2019, doi: 10.1109/ACCESS.2019.2960449.
Parenthetical citation: (Liu et al., 2019)
Narrative citation: Liu et al. (2019)

N. Ahmad, P. A. Laplante, J. F. DeFranco and M. Kassab, "A Cybersecurity Educated Community," in IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 3, pp. 1456-1463, 1 July-Sept. 2022, doi: 10.1109/TETC.2021.3093444.
Parenthetical citation: (Ahmad et al., 2022)

Narrative citation: Ahmad et al. (2022)

R. Kozik, M. Choraś and W. Hołubowicz, "Packets tokenization methods for web layer cyber security," in Logic Journal of the IGPL, vol. 25, no. 1, pp. 103-113, Feb. 2017, doi: 10.1093/jigpal/jzw044.
Parenthetical citation: (Kozik et al., 2017)
Narrative citation: Kozik et al. (2017)

S. Goel and B. Nussbaum, "Attribution Across Cyber Attack Types: Network Intrusions and Information Operations," in IEEE Open Journal of the Communications Society, vol. 2, pp. 1082-1093, 2021, doi: 10.1109/OJCOMS.2021.3074591.
Parenthetical citation: (Goel & Nussbaum, 2021)
Narrative citation: Goel and Nussbaum (2021)

W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq and M. K. Khan, "Comprehensive Review of Cybercrime Detection Techniques," in IEEE Access, vol. 8, pp. 137293-137311, 2020, doi: 10.1109/ACCESS.2020.3011259.
Parenthetical citation: (Al-Khater et al., 2020)
Narrative citation: Al-Khater et al. (2020)

Z. Yu, Z. Kaplan, Q. Yan and N. Zhang, "Security and Privacy in the Emerging Cyber-Physical World: A Survey," in IEEE Communications Surveys & Tutorials, vol. 23, no. 3, pp. 1879-1919, thirdquarter 2021, doi: 10.1109/COMST.2021.3081450.
Parenthetical citation: (Yu et al., 2021)
Narrative citation: Yu et al. (2021)

Z. Zhan, M. Xu and S. Xu, "Characterizing Honeypot-Captured Cyber Attacks: Statistical Framework and Case Study," in IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1775-1789, Nov. 2013, doi: 10.1109/TIFS.2013.2279800.
Parenthetical citation: (Zhan et al., 2013)
Narrative citation: Zhan et al. (2013)