

Cyber Insight: An Intelligent E-Learning Platform for Enhancing Digital Education

Ali Alfiya Nizam

Department of Science and Technology, G.H.Raisoni Skill Tech University, Nagpur, India

Abstract

Cyber Insights is a website that teaches people about programming and cybersecurity. It is made to help people learn about safety. Cyber Insights has courses that're easy to understand for people who are just starting out and for those who already know a little bit about programming and cybersecurity. Cyber Insights teaches programming languages like C, C++, Java and Python. It also teaches about cybersecurity topics like network security, cryptography and threat management.

As we are upgrading daily our education system is also upgrading and taking a new a way of learning. This new way of learning uses internet and combination of applications termed as “platforms”. These applications is built with programming languages and are software’s in nature this software make use of hardware for physical interaction with user. So this research paper seeks out to find out what are e-learning is meant to because the e-eLearning is gaining popularity day by day and has many users. There are several e-learning platforms available online. And will the e-learning based learning will be a better option in future than traditional way of learning

Keywords: E-Learning Platform, Online Education, Learning Management System (LMS), Web-Based Learning, Digital Learning, Educational Technology, Cloud-Based Education, Remote Learning.



This is an open-access article under the [CC-BY 4.0](https://creativecommons.org/licenses/by/4.0/) license

1. Introduction

E-learning is nothing but learning with the help of internet using device that poses hardware and software. And so, the platforms used for learning is nothing but e-learning platforms like Google meet, BYJU’S, JARO EDUCATIOON and much more. The term “e-learning” was use in 1999, at cbt systems seminar. And later numerous words place along began to grow in search of associate degree correct description like “online learning” and “virtual learning”. However, the principles behind e-learning unit of measurement well documented throughout history, and there's even proof that means that early styles of e-learning existed as approach back as results of the nineteenth century.

Social media is a way for people to communicate work together and share information in the digital age.

The study of networks is very interesting because it shows us patterns and relationships, between users and communities that we cannot see. Researchers use ideas from graph theory, sociology and game theory to analyze these connections and understand how information spreads and how groups of people interact with each other. This is called Social Network Analysis, which's a key part of

Computer Science and Engineering. It helps us understand how people interact with each other online. How they behave on the internet.

1.1 Motivation

People are learning, talking and sharing information in ways because of e-learning and social networking. Many online learning platforms are not very interactive do not offer learning paths and do not work well with communication tools that learners use every day. Social networks produce a lot of data that shows how people interact, work together and share information.

This information is not used as much as it could be in education-learning and social networking are changing education. Learners want to interact and learn in a personal way. They also want to use tools they already use. The data, from networks can help make education better. It can show what works and what does not.

This can help teachers and learners.

1.2 Contribution

The following is a list of the things that this paper is about:

1. We want to combine e-learning with networking to make learning more interesting for people.
2. We use methods to study how people interact with each other and share information, on these networks.
3. We made a place where people can learn together and talk to each other.
4. We use ideas from graph theory to understand how people learn online and make it better.
5. We think that learning is more effective when people are connected and work together as a community to learn things and we try to make that happen.

The platform is very flexible. Makes sure learning is just right for each person. For people who're new to this it teaches basic skills like spotting phishing scams making strong passwords and being safe online. This is really important for beginners. For pros Cyber Insights has more advanced courses on things like network security, cryptography and ethical hacking. These courses help them keep learning and moving up in their careers as the threat landscape changes.

The platform is intended to serve as a valuable resource for organisations looking to develop their workforce's cybersecurity skills by training all employees in every department on fundamental concepts of cybersecurity. Cyber Insights is delivered in an online, self-paced format, providing an interactive, hands-on experience, with quizzes, simulations, and real-time feedback to help all students achieve a more thorough understanding of essential cybersecurity principles.

Social network course encompasses surprising secrets which have been time and again revealed with the help of tools like graph theory, sociology, game theory, etc. The study of these graphs and revelation of their properties with these tools has been termed as Social Network Analysis. Category: Computer Science and Engineering.

1.3 Literature Review

However, despite advances in technology, many of today's classical electronic learning systems are still facing obstacles with respect to providing a design for interactive, practical, and secure environments in which to learn, particularly in the important areas of technical training, such as cyber security, and programming.

There have been a number of researchers who have looked at (cyber security) challenges to deliver online education systems. Ibrahim et al. [1], for example, wrote about the security risks associated with electronic learning systems as a result of weaknesses in both database management systems and user

authentication systems. Their research also highlights the importance of developing strong security mechanisms to protect sensitive academic data.

Anghel and Pereteanu [2] look at approaches to cyber security in electronic learning environments. Their research also suggests that developing secure channels of communication as well as having risk management strategies in place will help to reduce the risk from cyber threats, despite their convenience.

Hajný et al. [8] proposed structured frameworks and tools for developing cyber security curricula. Their research demonstrated the effectiveness of using a mixed-methods approach, including theoretical and practical training in order to create a successful and sustainable learning ecosystem.

Although all of these studies have contributed to our understanding of the challenges posed by online electronic learning systems, the majority of existing online learning systems are oriented towards developing either a structured

1.4 Problem Statement

The way we learn is changing because of technology. Online learning platforms are now very popular.. There are some problems with the way these platforms work especially when it comes to learning about technical things like programming and cybersecurity. Finally, these platforms do not use the technology to make learning more interactive and fun. They do not have things like dashboards secure ways to control who can access what and good ways to store and manage data. So, the main problem we are trying to solve is how to make a learning platform that's secure, flexible and interactive.

2. Related Work

2.1 Overview

E-learning platforms for programming and cybersecurity are pretty good at teaching theory. They often do not have enough hands-on activities. A lot of these systems just give you video lectures, notes and quizzes. They do not have interactive labs or simulations where you can actually try out what you have learned. This means that students can learn about cybersecurity. They have a hard time actually using that knowledge to do things.

Some research papers talk about how important it's to have practical things like virtual labs and exercises in online learning. These things help you connect what you learn in class to life which is especially important for things like cybersecurity. Looking at these ideas can help us figure out how to make eLearning platforms better by adding more interactive things for people to do. This way people can actually practice what they learn, which is really important, for programming and cybersecurity.

2.2 Review of Literature

- Research by Ibrahim and his team in 2020 and Anghel and Pereteanu in 2020 talks about the cybersecurity challenges that e-learning platforms face. They say that we need to manage databases in a way control access safely and protect against threats like phishing and malware.
- Samonte and his team in 2023 came up with CyLearn, which's a web-based platform for learning about cybersecurity. The way it is structured and designed can give us ideas on how to improve the user experience organize courses and engage users in a way. CyLearn is an example of a web-based cybersecurity learning platform.
- Other researchers like Alharbi and his team in 2022 and Aldammagh and his team in 2022 explain how education is shifting from being teacher-centered to being learner-centered. They highlight the importance of e-learning models.
- Biswas and his team in 2007 and Noesgaard also discuss how to evaluate e-learning. What factors make it effective. During the COVID-19 period researchers like Khalil and his team in 2021 and Shivangi Dhawan showed how online learning became necessary and how it can be improved.

- More researchers like Sofie Bitter, Sedio and his team Alshboul and his team and Sheena and her team emphasize the importance of customizing courses making them accessible using blended learning and using technology to improve learning quality. Some studies focused on India by Gaikwad and his team and Zahor Ahmad show how e-learning is growing in the country. E-learning is growing in India.
- All these studies show that while e-learning has grown a lot there is still a need, for platforms that combine security, interactivity, personalization and practical experience.

TABLE I

Reference	Heading	Year	Summary	Task/Focus
Alharbi et al.	Acceptance of E- Methods	2022	This paper is about what makes people accept E-Learning Methods	The authors also think about how to make the online experience better for learners.
Aldammagh et al.	Adoption of E-Learning	2022	This one is about the history of E-Learning and how people come to accept it.	The authors look at models that help us understand why people like or do not like E-Learning.
Pradipta Biswas et al.	Evaluation Standards and Effectiveness	2007	The authors of this paper think about how to evaluate E-Learning.	They want to know if E-Learning is working well for students and teachers
Sofie Bitter et al.	Benefits of Blended Learning	2016	The authors talk about combining offline learning.	They think this mix is good, for education. It helps learners in ways.
Khalil et al.	The Impact of COVID on Education	2021	This paper is about how COVID affected E-Learning.	The authors think COVID will help E-Learning in the run. They believe E-Learning will be good for education.

2.3 E-Learning Statistics

In higher education, eLearning is increasingly popular. Post-secondary education students tend to be more interdependent. Some work full-time while others are part-time. Parents with children also play a role. The fact that eLearning can be self-paced in general makes it more convenient for students than the traditional chalk and a-board method. Reasons for Choosing E-Learning by Students

1. The figure presents the key factors influencing students to choose e-learning platforms
2. Affordability (55%) is the most important reason for selecting e-learning.

3. School accreditation (41%) is the second major factor considered by students.
4. Specializations within the degree (29%) and institutional reputation (28%) also play significant roles.
5. Course content (27%) and quality of faculty (20%) moderately influence student decisions.
6. Factors such as time to complete the program (18%), total number of courses (15%), flexibility of online/on-campus options (13%), and location (8%) have comparatively lower impact.
7. Overall, financial benefits and institutional credibility are the primary drivers behind students' preference for e-learning.
8. Source: Market.us Scoop.

Reason for Choosing E-learning by Students

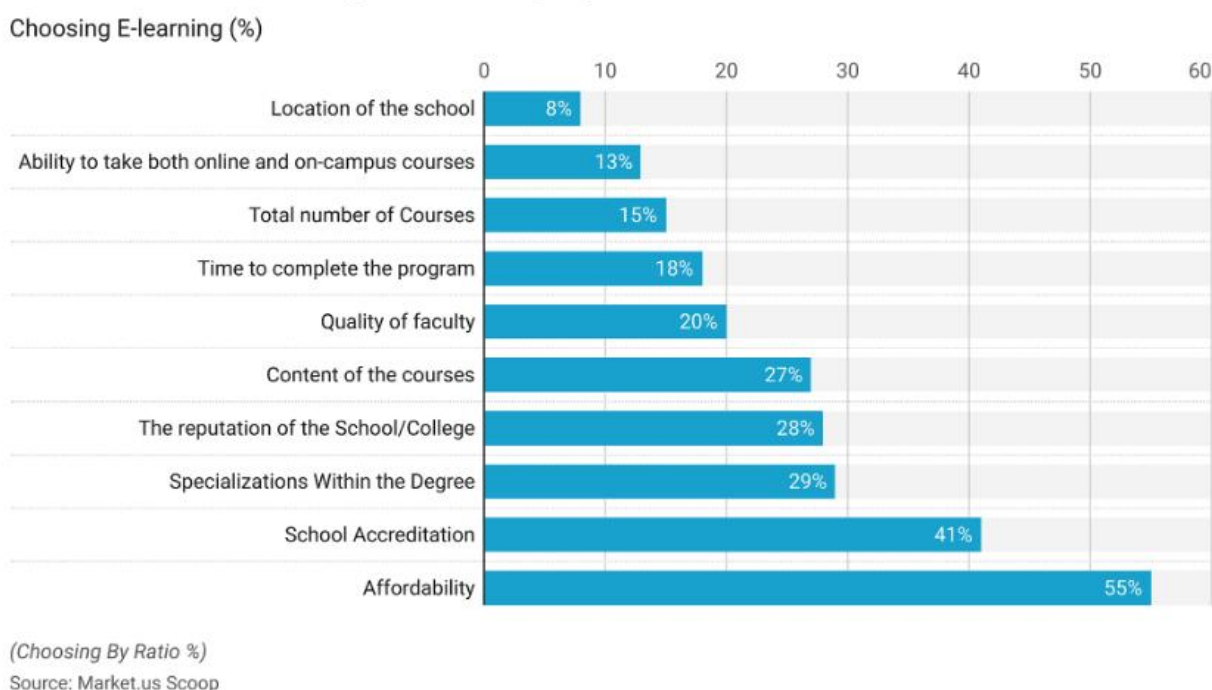


Fig.1. Choosing E-learning by Student

3. Research Methodology

We started our work by constructing a basic backend foundation, and we then tested the entire backend foundation with Postman. After we had finished testing the backend foundation, we moved on to developing the frontend of the application, which was developed to better reflect the overall model of the application and to allow easier use by end users.

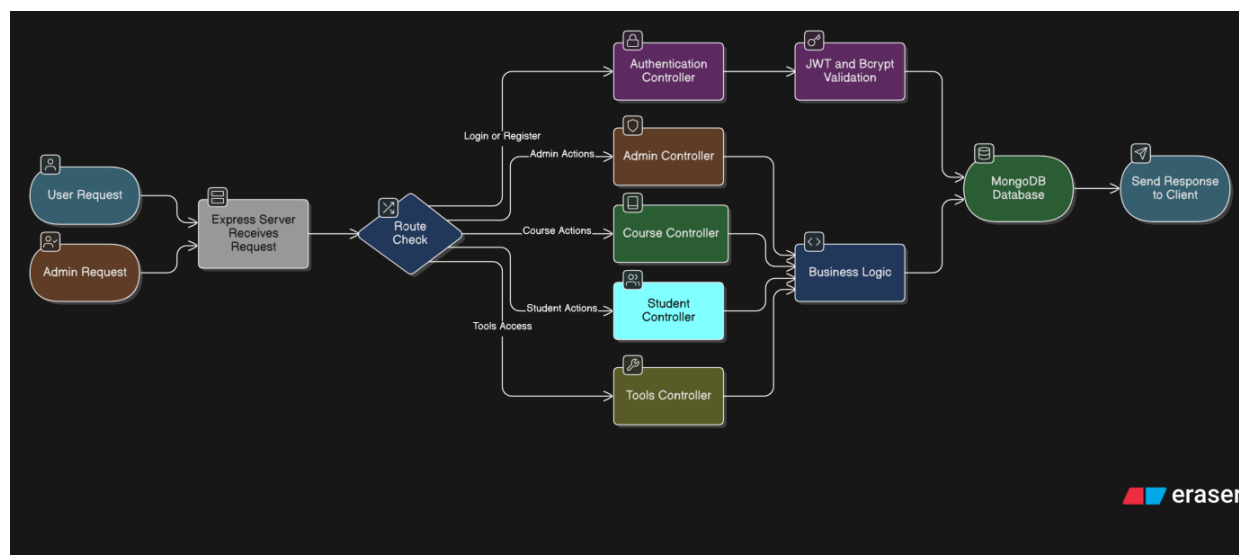


Fig.2. Backend Request Handling and Controller Architecture

Our process starts with two things: User Request and Admin Request. These are like messages from people using the system. The Express Server gets all these messages first. It is like the brain of the backend. The Express server does a things: it gets HTTP requests looks at the data and sends the requests to the right places. This helps keep everything between the client and server.

This picture shows how the backend of the system works. When a user or admin sends a message the Express server gets it. Checks where it needs to go. It is like looking at a map to figure out where to send the message. The message could be for things like logging in managing courses working with students doing admin tasks or using tools. Based on where the message needs to go it gets sent to the controller.

The controller helps out in many different ways. There are controllers for different uses such as: Authentication Controller for log in and Registration, Admin Controller for Administrative needs, Course Controller for Course needs, Student Controller for Student needs and Tools Controller for use of Tools, etc. All controllers are able to process their actions in order to ensure the message itself is processed properly.

We also use Bcrypt for secure password storage and JWT for keeping users logged into our website; When the controller completes its duty, it uses the MongoDB Database to obtain or store the required information (data). Once that has occurred, we return the appropriate response back to the client; Once again, this ensures data is secure and processed correctly as well as providing seamless communication between client, server and data.

The message gets sent to one of the controllers based on where it needs to go.

- The Authentication Controller handles logging in and registering.
- The Admin Controller does admin tasks.
- The Course Controller does course things.
- The Student Controller does student things.
- The Tools Controller does tool things.

This is the part of the application where the main work gets done. The data that has been processed is then stored in. Retrieved from the MongoDB Database. We chose MongoDB because it is flexible and works with JavaScript. We use plans to keep track of users, courses, tools and what people are doing. This helps us keep everything organized.

By using layers controller-based routing, secure authentication and structured database management the system works well. Is also very secure. This makes it a good choice for schools and, for world use. The Business Logic layer and MongoDB Database work together to make sure the application is secure, modular and scalable which is what we want for our web application design.

How it was built:

Step 1— Project Planning and Requirements Gathering

The project started with talking to the people involved to figure out the goal: creating an interactive e-learning platform for programming and cybersecurity with hands-on tools. We found out what the users needed for three groups students, admins and learners who use tools. We made a list of what the platform had to do like letting people register log in access courses see their dashboard and use cybersecurity tools. We also decided on the details choosing the MERN stack, which includes React, Node.js, Express and MongoDB and the MVC architecture to keep everything organized

We defined three user roles:

- **Admin** – this person is in charge of courses, students and tools
- **Student/Learner** – this person uses the platform to access courses and cybersecurity tools
- **System** – this is the part that handles logging in storing data and processing information

We wrote down all the things the platform had to do like logging in seeing the dashboard accessing courses using tools and tracking progress.

Step 2 — System Design and UI/UX Planning

Low-fidelity wireframes were created using design tools to visualize page layout and user flow

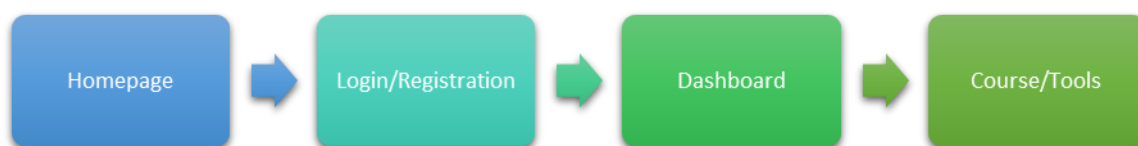


Fig.3. User Flow Diagram

These designs were improved into high-fidelity mockups after usability feedback. Focus was given to:

- Easy navigation
- Clean dashboard
- Accessibility of tools and courses
- User-friendly experience for beginners.



Fig.4. Home Page

Step 3 — Frontend Development (React.js)

The Cyber Insights frontend was built as a Single Page Application using React.js. This was done to make navigation fast render pages dynamically and provide an experience for users without reloading the entire page.

React's component-based design helped us build the UI in parts. We designed parts like the Header, Footer, Forms, Cards and Dashboard widgets as components. This approach made sure that these parts looked and worked the same across all pages. It also helped reduce code duplication. We focused on making Cyber Insights frontend user- efficient by utilizing React.js for a Single Page Application. Cyber Insights use of React.js enabled an efficient frontend.

The React.js component-based architecture made the Cyber Insights frontend more consistent and reduced duplicated code. Navigation was a breeze with React Router. It let users switch between pages like Homepage, Login/Register, Dashboard, Courses and Tools without any hassle. We added a protection mechanism for routes. This way only users who were logged in could access pages, like the dashboard and tools. If someone wasn't authenticated, they couldn't access those pages. Instead, they were sent to the login page.

The website was made to work on all kinds of devices like computers, tablets and phones. We used Bootstrap and Material UI to make this happen. We also made sure that people who are not good, with computers can use the website easily.

We did a few things to make the website work well:

- We made parts of the website that can be used again and again like the bottom parts and the forms that people fill out.
- We used React Router to help people move around the website.
- We used Context API and Redux to keep track of what's happening on the website.
- We used Axios to talk to the backend of the website.

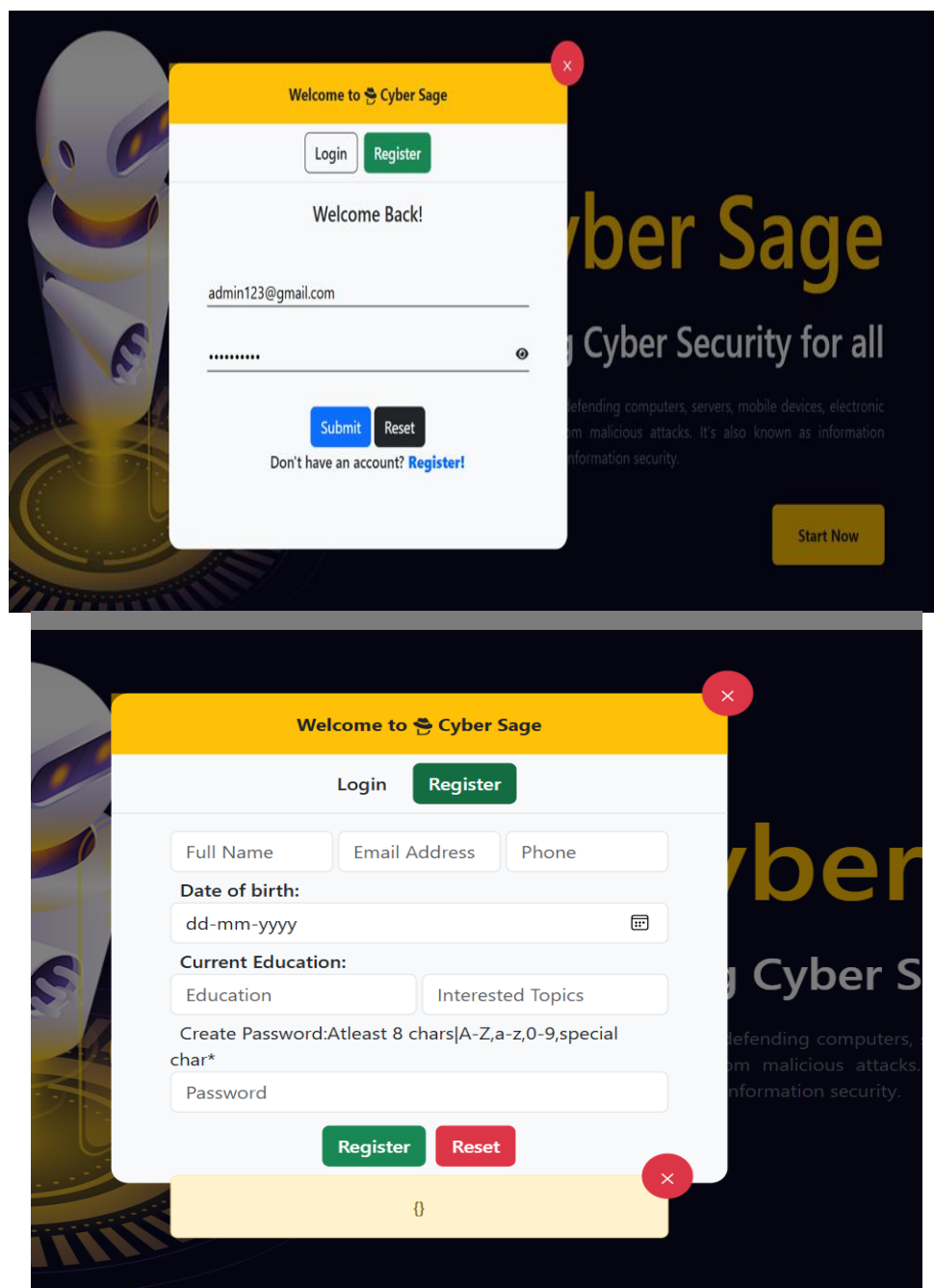


Fig.5. Login Page and Registration Page

Step 4 — Backend Development (Node.js + Express.js)

This pattern is really helpful because it separates the application into parts like models which are basically database schemas, controllers which have the business logic and routes which are the API endpoints. This makes the code easy to understand and work with. It is also scalable and easy to maintain. We made RESTful APIs to handle things like user information, courses, progress tracking, things that admins need to do and cybersecurity tools. We had controllers like the Auth Controller and the Admin Controller and the Course Controller and the Student Controller and the Tools Controller. Each of these controllers did jobs. They got requests applied the business logic and then talked to the database using the models. The backend server was created using Express.

Main tasks:

- Creating RESTful APIs for users, courses, and tools

- Route handling and controllers (Auth, Admin, Course, Student, Tools)
- Middleware for logging, CORS, JSON parsing, and authentication
- Centralized error handling.

The backend was tested initially using **Postman** before frontend integration.

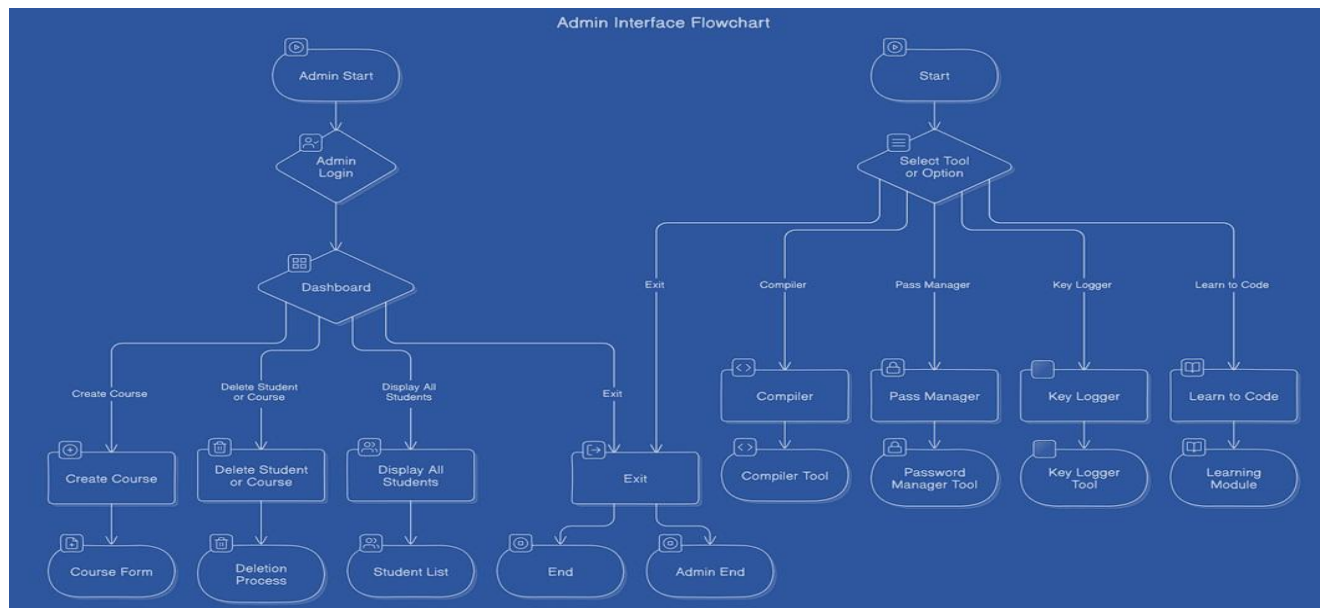


Fig.6. Flow chart for project process

Step 5 — Database Design (MongoDB)

MongoDB schemas were designed using Mongoose for:

- Users
- Courses
- Progress tracking
- Tool usage data

We made sure to include all the things like creating, reading, updating and deleting data, validations, indexing, pagination and data seeding.

Step 6 — Building Security and Authentication Features into Our Website Building security into the website is critical for users. Therefore:

- Use bcrypt to hash passwords for security.
- Use JWT tokens for managing user sessions.
- Tokens have an expiration date.
- We utilize role-based authorization - users are assigned roles that determine what actions they can take with their accounts.
- We use a secure communication channel between the client and the server.

Step 7— Integration of Cybersecurity Tools

Special modules were added:

- Compiler for coding practice
- Password strength tester

- Keylogger simulation
- Encryption/Decryption practice tool

These tools provide hands-on cybersecurity learning in a safe environment.

Step 8— Testing and Quality Control

Three different tests were conducted.

- The unit tests will be done using Jest and Supertest.
- Testing the interface (frontend) and the server (backend) together.
- Testing the system with real users and stakeholders to get User Acceptance Testing?
- Data will be used at each of these stages as guidance to allow for continual enhancement of the system (Agile methodology).

Step 9 — Deployment

- Backend deployed on Heroku/AWS
- Frontend deployed on Vercel/Netlify
- MongoDB Atlas used for cloud database
- Environment variables secured for production

Step 10 — Documentation

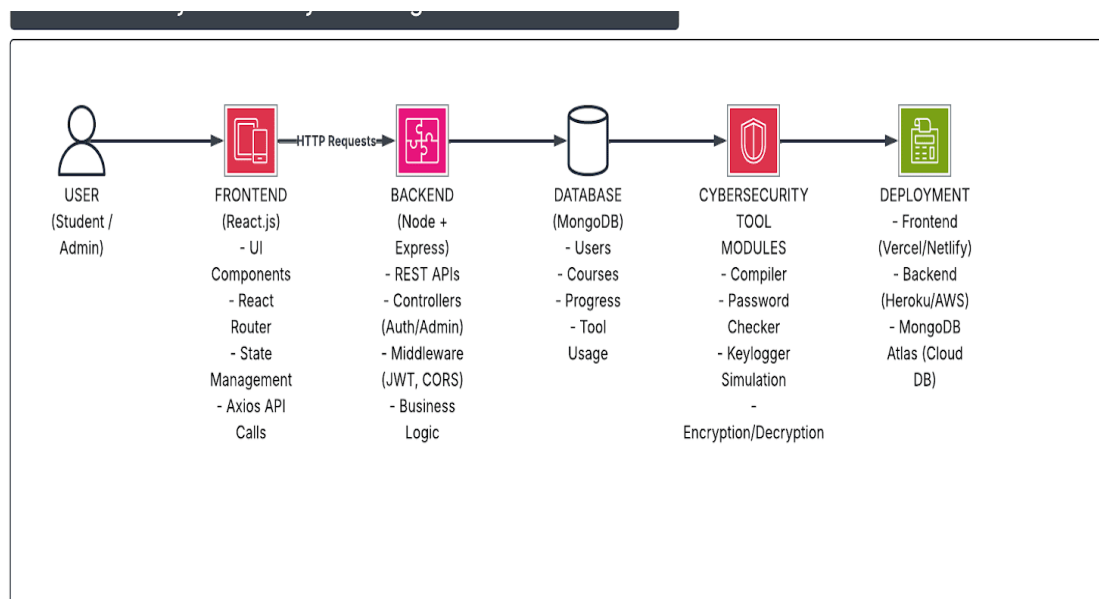
- API documentation using Postman/Swagger
- User manual for learners
- Code maintained using GitHub version control

Step 11 — Maintenance and Future Updates

- Performance monitoring and error logging
- Regular updates based on user feedback
- Scalability planning for more users and courses

Overall Website Flow (How it Works)

1. User visits **Homepage**
2. Registers or logs in
3. Redirected to **Dashboard**
4. Accesses Courses or Cybersecurity Tools
5. Progress is stored in database
6. Secure logout after Session

**Fig.7. System Architecture**

4. Conclusion And Future Work

4.1 Conclusion

This research collated and assessed the traditional and modern approaches to online learning; compared these traditional and modern learning methods to Cyber Insight's proposed new model of online learning; and evaluated the advantages and disadvantages of existing e-learning systems as they relate to flexibility, accessibility, customisation, and the ability to develop practical skills.

Based on this comparative evaluation, the project created a learner-friendly model to improve upon existing gaps identified by other e-learning systems. Most existing online education providers offer structured classes but do not give their users the flexibility to access the content/topics/lectures they need on an "as needed" basis (e.g., immediate need).

The proposed model of Cyber Insight suggests granting the user the option to request and view content/lessons without having to commit to a complete course experience. Furthermore, Cyber Insights provides users with an opportunity to have a freelancing style of teaching experience by allowing those who have knowledge/experience of a particular subject area to share their knowledge and experience with others.

This opportunity for educators and learners creates a collaborative and open environment for continuing education, enhances the learning process of both group and individual building of skills for both educators and learners, and promotes an increased interest in and commitment to education. In a few years' time, current computer technology will be outdated. Clearly, the availability of broadband technology will increase the online learning options by making use of videoconferencing, advanced animation techniques, and virtual scientific laboratories. Electronic books have become more prevalent.

Learning opportunities will expand further (Antonucci and Cronin, 2001). There is no doubt that e-learning has an important role to play across all business sectors. In addition to its cost-effectiveness, its main advantages are its flexibility, its convenience to users, its wide reach, its easy accessibility, its consistency and its repeatability. The objectives of e-learning are dependent on the quality of the teaching process and the effectiveness of online access.

Several script languages and Internet-

oriented languages have been used to embed interactivity into Web pages (Hall, 1998), including Java and JavaScript. Among them, Java is the most powerful tool to make Web pages interactive. This is because it is a proper object-oriented language, platform-free, and has more functionality than its competitors.

4.2 Future Work

The Cyber Insights platform is really good. There are some things that can be done to make it even better and more useful for people.

1. Advanced Cybersecurity Modules

In the future the platform can include advanced topics like:

- Penetration Testing
- Ethical Hacking
- Digital Forensics
- Cloud Security
- Malware Analysis
- Secure Coding Practices

This will make the Cyber Insights platform completer and more relevant to the industry.

2. AI-Based Personalized Learning Paths

Now users have to choose their courses themselves. But in the future the platform can use Artificial Intelligence to look at how usersre doing how fast they are learning and what they are interested in and then suggest a personalized learning path for them. This will make the learning experience fun and effective.

3. Industry-Based Certification Programs

The platform can offer certification programs that are recognized by the industry like CEH or CompTIA Security+. This will make the platform more credible and useful for peoples careers. Users can get certificates when they complete a course.

4. Real-Time Collaborative Learning

Some other things that can be added to the platform are:

- Discussion forums
- Live sessions to clear up doubts
- Working with users
- Virtual labs where users can work together

This will make it easier for users to learn from each other.

5. Mobile Application Development

The platform is currently only available on the web.. A mobile app for Android and iOS can make it easier for users to access the platform from anywhere.

6. Cloud-Based Virtual Labs

The platform can include labs that are based in the cloud, where users can practice penetration testing in a safe environment.

7. Performance Analytics Dashboard for Admins

The administrators can use a dashboard to see how users are doing, like:

- How courses they have completed
- How engaged they are
- What tools they are using
- How the system is performing

This information can help make the platform better in the future.

To sum it up the future of the Cyber Insights project is about making it better and more useful for people.

- We can add features to the platform in the future.
- We can give users advanced software for managing their learning with more facilities.
- We will make the platform available online so people can access it from anywhere in the world
- We will use load balancers to make sure the system can handle a lot of users
- We will create a master and slave database structure to make the database more efficient
- We will implement a system so we can save the code and database in case something goes wrong.

This research looked at how people learn online and proposed a new model that combines structured education with flexibility and opportunities for collaboration. The Cyber Insights platform brings together education with new and innovative elements like being able to access lectures on demand and learn from freelancers.

The platform has a foundation, with a secure system, practical learning tools and a design that can grow with the number of users. With development and integration of new technology the platform has the potential to become a leading digital learning ecosystem.

The E-Learning website is an working website that allows users to register, access course materials and run code examples. One of the things about this application is that users can run codes and see the results of different networks using an online compiler, which helps them develop practical knowledge of the concepts they learn from the notes and video lectures.

Users also have access to the course materials once they register on the website for free. The main goal of the application is to give users knowledge of Social Networks along, with notes and video lectures.

5. References

1. I. Ibrahim, S. Karabatak, and A. A. Abdullahi, "A study on cybersecurity challenges in e-learning and database management system," in *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 2020, pp. 1–5.
2. M. Anghel and G. C. Pereteanu, "Cyber security approaches in e-Learning," in *INTED2020 Proceedings*, 2020, pp. 4820–4825.
3. M. Tisma and J. Andric, "Importance of cyber security awareness and e-learning motivation for cyber security in reshaping the education," *Journal of Information Systems & Operations Management*, vol. 15, no. 2, pp. 284–296, 2021.
4. R. Beuran, K. Chinen, Y. Tan, and Y. Shinoda, "Towards elective cybersecurity education and training," Japan Advanced Institute of Science and Technology.

5. M. J. C. Samonte, K. N. U. Banganay, K. E. Fernandez, and J. N. D. Jamena, "CyLearn: An assistive web-based e-learning system for cybersecurity skills course," *International Journal of Information and Education Technology*, vol. 13, no. 6, 2023.
6. M. Shivapurkar, S. Bhatia, and I. Ahmed, "Problem-based learning for cybersecurity education," *Journal of The Colloquium for Information Systems Security Education*, vol. 7, no. 1, pp. 6–6, 2020.
7. T. Ghosh and G. Francia III, "Assessing competencies using scenario-based learning in cybersecurity," *Journal of Cybersecurity and Privacy*, vol. 1, no. 4, pp. 539–552, 2021.
8. J. Hajny, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta, and R. De Nicola, "Framework, tools and good practices for cybersecurity curricula," *IEEE Access*, vol. 9, pp. 94723–94747, 2021.
9. D. Tang, C. Pham, K. Chinen, and R. Beuran, "Interactive cybersecurity defense training inspired by web-based learning theory," in *2017 IEEE 9th International Conference on Engineering Education (ICEED)*, 2017, pp. 90–95.
10. Y. T. Sung, K. E. Chang, and W. C. Yu, "Evaluating the reliability and impact of a quality assurance system for E-learning courseware," *Computers & Education*, vol. 57, no. 2, pp. 1615–1627, 2011.
11. S. Furnell and N. Clarke, "Power to the people? The evolving recognition of human aspects of security," *Computers & Security*, vol. 31, no. 8, pp. 983–988, 2012.
12. M. Bishop, *Computer Security: Art and Science*, 2nd ed. Boston, MA, USA: Addison-Wesley, 2018.
13. W. Stallings and L. Brown, *Computer Security: Principles and Practice*, 4th ed. Pearson Education, 2018.
14. Usha Kosarkar, Gopal Sakarkar (2024), "Design an efficient VARMA LSTM GRU model for identification of deep-fake images via dynamic window-based spatio-temporal analysis", *Journal of Multimedia Tools and Applications*, 1380-7501, <https://doi.org/10.1007/s11042-024-19220-w>
15. Anupam Chaube, Usha Kosarkar "Enhanced Deep Learning-Based Feature Analysis for Copy-Move Forgery Detection", 2024 *Journal of Information Systems Engineering and Management*, 9(4s) e-ISSN:2468-4376, <https://www.jisem-journal.com/>