JOURNAL OF MULTIDISCIPLINARY SCIENTIFIC KNOWLEDGE

Vol. 01, No. 01

Edu-CyberSphere: Design of a Multimedia-Integrated Discussion Platform for Cybersecurity Learning

Dr. M V N Srujan Manohar[1*], Dr. G Anand Kumar[2], Neeraj Kundarapu[3], Maram Shanmukh Pavan Reddy[4], Aluru Ramesh Khanna[5], Vankayala Anil Santosh[6]

Received:- 01/02/2026, Revised:- 11/03/2026, Accepted:- 19/03/2026, Published:- 26/03/2026

Abstract

Edu-CyberSphere is a future-proof multimedia discussion forum and learning platform in the field of cybersecurity and associated emerging fields, such as the Artificial Intelligence and Machine Learning (AIML), Internet of Things (IoT), Data Science, Information Technology (IT), and Computer Science Engineering (CSE). This platform does not only offer the usual cybersecurity education but also enables users to discover, share resources, and conduct dynamic discussions in a wide range of technological domains. One such feature of Edu-CyberSphere is that it combines the practical cryptography tools that are available on the homepage and therefore allows real-life use of encryption, decryption, hashing and digital signatures. These interactive tools are able to serve the user in any level and increase experiential learning. An obfuscator of code is also provided to protect the contributions of users even further, and thus the anonymity and security of the source code is guaranteed in accordance with the principles of zero-trust security.

The multimedia enabled system forum offers a very flexible and secure authentication system with email, phone, social network and biometric options of logging in. This is done by using advanced security measures such as high-level encryption and verification to ensure that user data is not accessed by unauthorized users. The incentive to engage with the community is provided by an extensive reward system that grants points and badges according to the participation and other useful contributions to the community, which leads to the creation of an active, established user base.

Personalization options enable the users to configure the themes of forums and use dynamic, animated user tags, thus increasing profile identity and interaction with the rest of the community. The threads that are core are startup incubation, freelance skill-sharing and forums to discuss the stock and crypto market in specialized forums. In aggregate, Edu-CyberSphere delivers innovative functionalities that promote security, creativity, networking, professional development, and an enriched user experience for today's technology-driven learners and practitioners.

Keywords: Cybersecurity education, multimedia forum, cryptography tools, interactive learning, authentication, code obfuscation, zero-trust security, gamification, personalization, community engagement.

[1*]School of Engineering, Department of IoT, Malla Reddy University Hyderabad, India.
Email Id: srujanmanohar.edu@gmail.com
[2]School of Engineering, Department of IoT, Malla Reddy University Hyderabad, India.
Email Id: anandlife@gmail.com
[3]School of Engineering, Department of IoT, Malla Reddy University Hyderabad, India.
Email Id: theneerajkundarapu@gmail.com
[4]School of Engineering, Department of IoT, Malla Reddy University Hyderabad, India.
Email Id: pavanreddy576.pr@gmail.com
[5]School of Engineering, Department of IoT, Malla Reddy University Hyderabad, India.
Email Id:rameshkanna.aluru@gmail.com
[6]School of Engineering, Department of IoT, Malla Reddy University Hyderabad, India.
Email Id: anilsantosh1984@gmail.com

Corresponding Author: Dr. M V N Srujan Manohar
Email Id: srujanmanohar.edu@gmail.com

1. Introduction

The growing sophistication of cyber threats and the unique pace of digital technologies development has contributed to cybersecurity education becoming one of the urgent needs of contemporary academic and professional communities. The conventional methods of cybersecurity education are usually based on theoretical education and less interaction, which lead to a lack of practical learning and engagement by learners. Online learning environment research suggests that the traditional online learning forums are characterized by the basic issues of passive interaction and lack of interactivity [1]. There is also the consideration of factors affecting the adoption of e-learning which indicates that learning platforms should be flexible and user friendly so as to enhance effectiveness and acceptance among the learners [2].

Additionally, the existing systems of online education also stress the significance of organized and interactive learning tasks to improve the knowledge building and satisfaction of learners [3]. Online learning communities are also important in helping to develop interaction, collaboration, and constant engagement between the learners [4]. With the recent integration of new areas of information security with Artificial Intelligence, Machine Learning, the Internet of Things, and Data Science, the need to have holistic platforms to facilitate both interdisciplinary education and application development is on the rise.

Edu-CyberSphere is suggested to be a more unified, practical, and interdisciplinary cybersecurity learning platform that would overcome these shortcomings. The platform is based on interactive learning and discussion group environments to facilitate interaction and skill-building. It focuses on active learning that is structured, with practical exposure and community-based knowledge transfer, unlike in the traditional forums. Through the combination of the interactive learning principles and the collaborative digital ecosystem, Edu-CyberSphere will address the gap between the theoretical knowledge and its practical implementation as well as allow promoting innovation, participation, and continuous learning in cybersecurity education.

2. Purpose

2.1. Addressing the Limitations of Traditional E-Learning Forums.

This is because the main aim of Edu-CyberSphere is to overcome the drawbacks that are normally witnessed in the traditional e-learning forums, especially passive learning, lack of interaction, and inability to support active learning among learners. Students and their perception of using online forums shows that although this tool can facilitate the discussion, it cannot be effective in maintaining meaningful engagement when used in a traditional format [5]. Edu-CyberSphere is thus developed to go beyond the simple question-answer format by developing a more interactive and learner-centered space that promotes active participation and knowledge sharing.

2.2. Maintaining Integrating Practical, Hands-On Skill Development

By introducing practical exercises directly into the gamified learning environment, the project will fill the gap in the theoretical knowledge and its practical application that is critically important in the field. The platform also has interactive capabilities such as built-in cryptography tools and a source code obfuscator which enable the students to do real-life work. This will translate abstract ideas into concrete problems, which is the effectiveness of serious games and customizable cyber ranges in developing tangible cybersecurity skills.

2.3. Providing a Model for Broader Technical Education

Edu-CyberSphere is the conceptual framework, which can be applied to the implementation of the interactive and gamified learning strategies into the broader technical spectrum. Even though the platform is dedicated to cybersecurity, the concepts of its design, such as the application of engagement in the learning process and involvement of the user can be transferred to other technical fields. The knowledge and memorization in the complex fields of the subjects have been established to be improved by the learning models which are grounded in gamification and the models can be expanded to wider learning contexts [6]. This points to the possibility of the platform being a scalable framework of interdisciplinary technical education.

2.4. Enhancing Learning and Motivation Through Gamification

One of the main goals of Edu-CyberSphere is to increase student motivation and engagement by using the system of gamification methods. As it has been shown, gamified methods may considerably enhance the issue of security awareness, participation, and learning outcomes through the integration of such concepts like rewards, challenges, and interactive feedback [7]. Following these principles, the platform combines such features as points, badges, leaderboards, and challenges to make the learning experience more exciting and motivating to users.

3. Literature Survey

Recently, the trend in cybersecurity education has shifted towards interactive and practice-based methods of learning to enhance learner engagement and conceptual learning. Serious games have also become a useful teaching tool by adding simulation-based challenges and learning immersiveness that makes cybersecurity concepts more approachable and interesting [8]. Similarly, gamification-related strategies have been reported to enhance technical skills of the learners like network security by incorporating rewards, progression, and interactive learning into the learning process [9].

3.1. Gamification in Cybersecurity Education

Gamification is now recognized as a valuable approach to cybersecurity education to increase motivation, engagement and retention of complex ideas. An advanced analysis of gamification in the context of cybersecurity education shows that it is becoming increasingly significant when creating more efficient and learner-focused learning systems [10]. These results can justify the creation of platforms like EduCyberSphere that aim to make cybersecurity education more interactive and responsive to the needs of learners using structured game-based components.

3.2. Decentralized Learning Environments

Learning environments based on cybersecurity are becoming more practical and distributed in nature, and they promote collaboration, experimentation, and learner autonomy. Studies on the implementation of cyber range at varying levels of learning demonstrate that cyber range offers scalable, flexible learning opportunities of hands-on cybersecurity training and supports a wide range of learners [11]. This illustrates the importance of collaborative and practice-based platforms in enhancing technical preparedness and practicability in solving problems.

3.3. Privacy and Security in Learning Platforms

Security, accessibility, and effectiveness of the learning environments where learners work should also be taken into consideration in the design of cybersecurity learning platforms. Comparative study of the open-source cyber ranges indicates that architecture of the platform, usability, and design of implementation are all major determinants of education value and operational performance [12]. These results apply to sites such as EduCyberSphere, where secure and highly organized learning communities are a necessity in facilitating meaningful and reliable interaction between the user.

3.4. AI-Driven Insights and Adaptive Learning

All the reviewed studies indicate that the current state of cybersecurity education is moving towards more interactive, practical, and adaptive learning environments. The literature has serious games and gamified instructional approaches to cyber ranges and platform design structure, where the focus on learner-centred innovation in cybersecurity training is high. An understanding of EduCyberSphere in this larger development is as a platform concept that has been consistent with current technology to enhance the efficiency and access to cybersecurity education.

4. System Analysis and Design

The Edu-Cyber Sphere design is based on the development of a stable, safe, and interactive platform, which will overcome the limitations detected during the literature review. The system was created on a modular architecture in order to be scalable and easy to maintain. Authors and Affiliations.

4.1. System Architecture and Technological Stack

Edu-Cyber Sphere is designed on a client-server architecture based on the XenForo forum framework as the basic framework. The technological stack was selected due to its reliability, large community support and powerful feature base. The main development and test setup was done with the help of XAMPP that offers a combined server package.

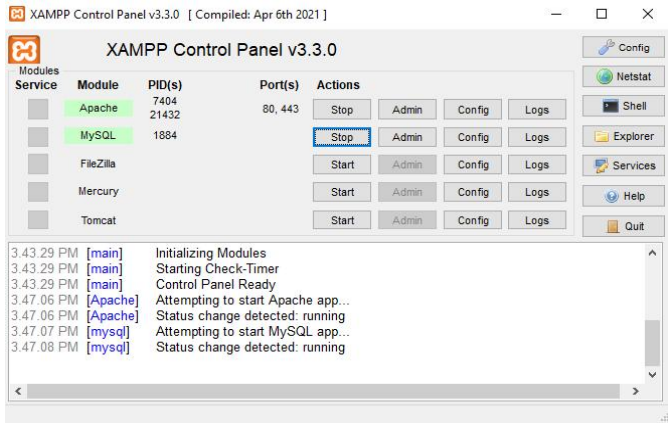

Fig. 1 Example of a figure caption.

The backend server is written in PHP, which is a server-side scripting language that is used to perform all business logic, user authentication, and database operations. The frontend is produced in the standard web technologie , HTML, CSS, and JavaScript in order to provide the responsive and interactive user experience on all the modern web browsers.

4.2. Database Design and Management

The system will rely on the MySQL relational database (maintained through HeidiSQL) to store user credentials, posts in forums, rewards and system configurations securely. The database structure is efficient, data integrity and security. The main user management table, xf_user, also has the fields of user identification, hashed passwords, secret_key and profile details as illustrated in Fig. 2.

Security is a primary consideration in the database design. In addition to password hashing, the system generates a unique secret_key for each user account.

Fig. 2 The database schema for the xf_user table as viewed in HeidiSQL, detailing user-related data fields.

4.3. Key System Modules and User Interface

The functionality of the platform is designed in modular units, each of which has its own definition and respective classes and roles. The modules are important such as Core Forum Engine, User Authentication, Backend Logic, Frontend Interface, and Specialized Learning Tools as shown in System class diagram.

i. User Authentication and Registration:

The site has a simple and secure registration process. The new users will be required to

fill the standard information and do a security check with the assistance of h Captcha to prevent the formation of automated spam accounts. The site also supports an easy registration by Discord, which targets the target group of technology enthusiasts (Fig. 3).

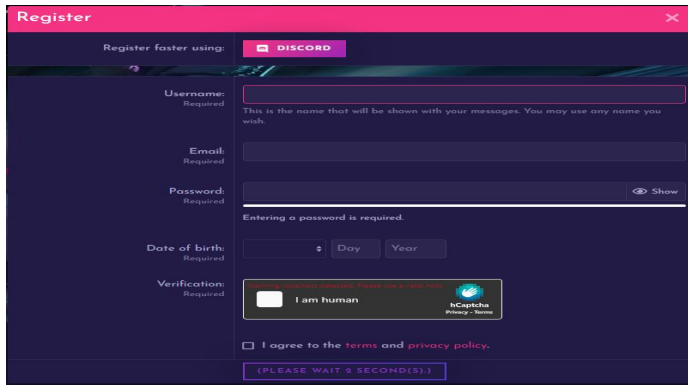

Fig. 3 The user registration interface, featuring required fields, hCaptcha verification, and an option for Discord integration.

ii. Community and Discussion Forum:

This is the main module of the system, which allows people to form threads, place answers, and participate in discussions on different technical issues. The interface is made to be clear and easy to interact with and create a collaborative learning atmosphere (Fig. 4).

iii. Practical Learning Tools:

The platform combines a specific module of Cryptography Ciphers to achieve practical learning. This aspect would give the user immediate access to a collection of useful encryption and decryption tools, which enables him/her to implement theoretical knowledge in the real-world setting (Fig. 5).

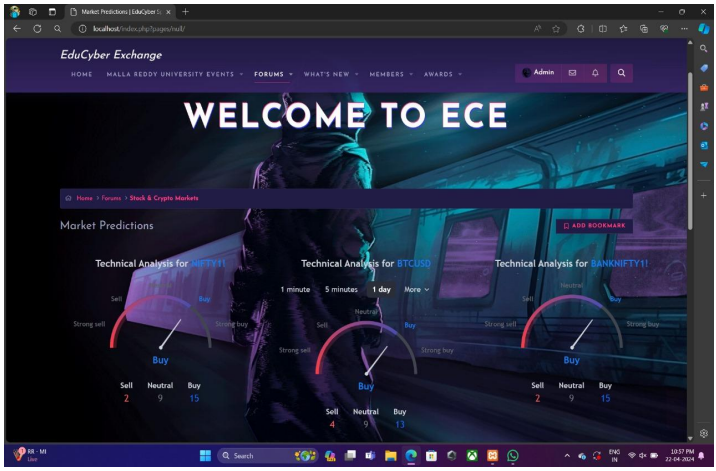

Fig 4. A typical discussion thread within the Edu-Cyber Sphere forum, showcasing user interaction.

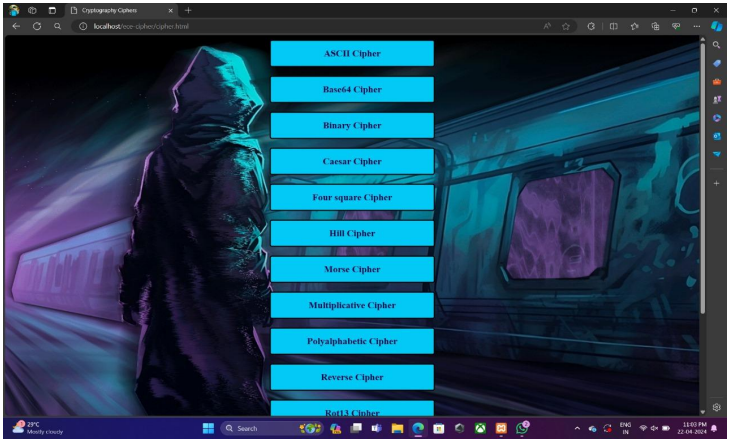

Fig. 5 The main menu for the integrated practical cryptography tools, offering a selection of different ciphers for users to experiment with

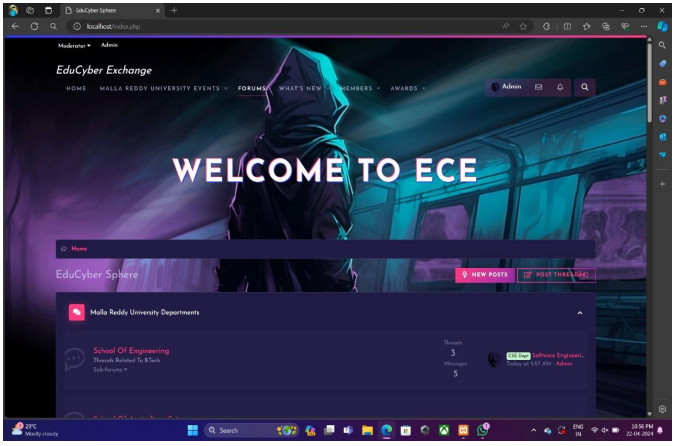

Fig. 6 The Market predictions dashboard, providing technical analysis indicators for various asset.

iv. Specialized Content Modules:

In addition to the usual discussion on forums, Edu-Cyber Sphere offers market analysis modules. They contain in-built widgets that display real-time stock and cryptocurrency data and technical analysis, broadening the platform to cover financial technology and market trends (Fig. 6 and Fig. 7).

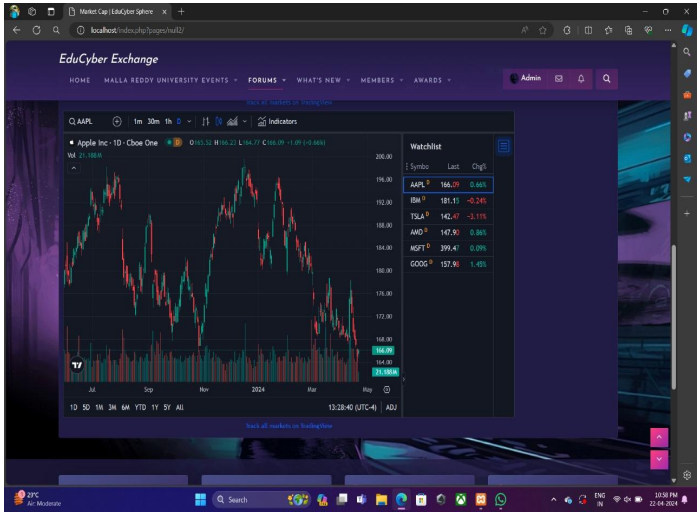

Fig. 7 A typical discussion thread within the Edu-Cyber Sphere forum, showcasing user interaction.

5. Analysis of Existing System

The overall analysis of the current e-learning tools focused on cybersecurity and other technical aspects of the area demonstrates the presence of several limiting factors. Although most platforms offer great educational opportunities, they do not in some of the aspects critical towards creating a highly motivated and skilled society. All these gaps were the main incentive to the creation of Edu-Cyber Sphere.

5.1. Narrow Topical Focus and Lack of Practical Application:

The majority of the traditional e-learning forums focus on a limited scope of conventional cybersecurity issues. They do not often cover any new and interdisciplinary topics, including Artificial Intelligence and Machine Learning (AIML), the Internet of Things (IoT), and Data Science. This narrowness does not capture the inter-relationship of contemporary technology. Moreover, a major drawback of these platforms is the lack of general integrated practical tools used in practical learning. People are also told about theoretical concepts but do not receive a setting where to apply them, which is a weakness that prevents the acquisition of realistic, practical skills.

5.2. Deficiencies in User Engagement and Motivation:

One of the major issues in current online learning communities has been the active use of the community as well as the fight against passive use. Most of the platforms have very simple interaction schemes and do not have the advanced functionality that can be used to encourage users. They are not inclined to use established pedagogical techniques like gamification, do not take advantage of rewards, recognition, and interactive challenges in order to generate a more interesting learning experience. This exclusion leads to a failure to have a dynamic community and may slow down the long-term user retention and acquisition of knowledge.

5.3. Inadequate Security and Professional Development Features:

In most of the current online forums, security is usually restricted to mere authentication systems that might not be adequate to secure user information and guarantee a secure environment. It is an especially important omission of a community that deals with cybersecurity. Moreover, these platforms do not often offer specific functions that would facilitate professional growth and cooperation in addition to mere discussion. The platform is usually not helpful in terms of career development and innovation in the community as there are no opportunities to allow users to participate in startup incubation, seek freelance work, or collaborate on projects.

6. Comparative Analysis

An overview of existing cybersecurity education tools and gamified learning systems, including SCORPION, SherLOCKED, and other cyber ranges, suggests that the majority of the systems concentrate on a limited set of subjects or do not effectively incorporate interdisciplinary technologies. Although these systems have good exercises, they usually lack the integration of practical tools, group discussion platforms, and professional growth functionalities all in one platform. Edu-Cyber Sphere fills these gaps through the provision of multimedia-based integrated forum that encourages active learning, gamified interest, and practical skills in the real world through integrated cryptography tools. The site also offers safe authentication, privacy through obfuscation of codes and market analysis, startup incubation and exchanging skills on freelance through specialized discussion threads. Its interdisciplinary nature, encompassing AIML, IoT, and Data Science in addition to cybersecurity, is also another advantage over the current platforms. All these characteristics make Edu-Cyber Sphere an all-encompassing and adaptable learning space that promotes not only the development of practical skills but professional readiness.

7. Methodology

7.1. System Architecture and Modules

Edu-Cyber Sphere architecture was designed in the object-oriented and modular design approach to provide scalability, maintainability, and security. The development lifecycle was led by a structured systems engineering approach, which included the requirement analysis, iterative design, implementation and testing. The review model includes both quantitative indicators (system performance, scalability, usability) and qualitative indicators (learning effectiveness, user satisfaction), which offers a solid foundation of platform impact evaluation. The system structure with the description of the main classes and their connections is shown in the class diagram in Fig. 8.

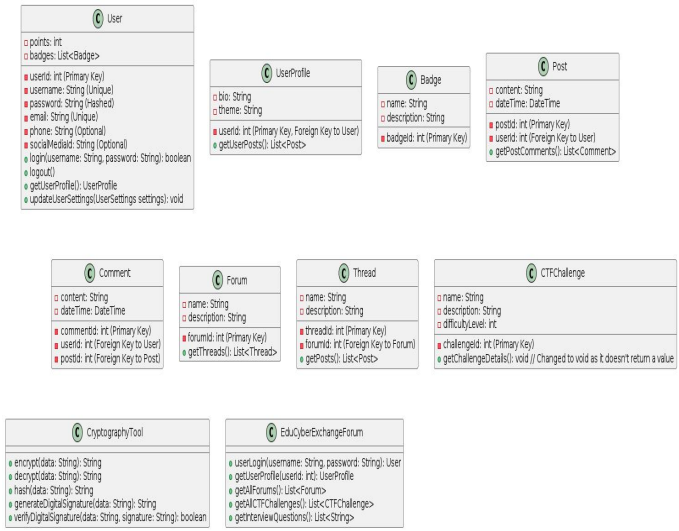

Fig. 8 Class diagram of the Edu-Cyber Sphere system, illustrating the key entities and their relationships.

Module 1: Core Forum and Community Engine

XenForo is the foundation of Edu-Cyber Sphere, as it is an extremely powerful and highly versatile community software that will be the heartbeat of all the interactions, through forums. This is displayed in the architecture in the classes of the Forum, thread, post and comment that govern the hierarchical form of the community discussion. Different discussion threads, posts made by the users, replies and the general structure of the community forums will be managed by this module. Based on an existing model, the system offers a cohesive and complete user base of participation, content management, and moderation.

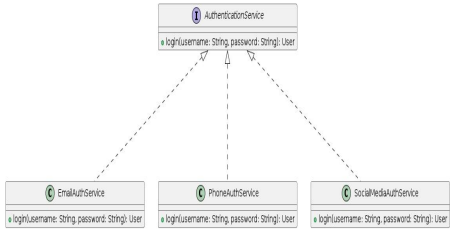

Fig. 9. The AuthenticationService interface and its concrete implementations, illustrating the use of the Strategy pattern for flexible user authentication.

7.2. Module 2: User Authentication and Security

The module also handles such critical events as registration and secure authentication of users. This design is founded on the Strategy pattern with an application of Authentication Service interface to allow a diversity of various but interchangeable authentication schemes. Fig. 9 illustrates that this scalable architecture offers concrete

email, phone and social media authentication. Such basic properties of user class as username, password Hashed, and email are provided, and the security is further restricted at the database level whereby every user is provided with a secret key unique to him/her and is generated by the system. This protocol offers a lot of security to user sessions and sensitive operations which is the best practice regarding a secure online community.

7.3. Module 3: Backend Logic and Database Management

The logic behind the back end is the server side functionality of the system and makes all exchanges between the user and the database. The back office is built on PHP and it runs on an Apache server in a XAMPP configuration. It is also linked to a MySQL relational database that securely stores and retrieves all the platform data, and is represented by the classes on the architecture diagram (e.g., User, Post). The database is managed using HeidiSQL which allows easy schema design and querying the data and guarantees the integrity and high performance of the system.

7.4. Module 4: Frontend User Interface and Engagement

The frontend interface will be user friendly and visually appealing to the user in order to communicate with the system. The UI has been developed in standard web technologies (HTML, CSS, and JavaScript) and is made responsive and user-friendly. The module is tasked with the responsibility of rendering the information handled by the backend classes (i.e. showing a user their UserProfile or their Badges). It also involves the introduction of the gamification and engagement strategy, the control of the visualization of the rewards system (points and badges) and other dynamic components that stimulate the active involvement in the community.

7.5. Module 5: Specialized Content and Learning Tool Integration

The module includes the combination of specific, specialized features, which are symbolized by such classes as CryptographyTool and CTF Challenge. The CryptographyTool class contains the functions to do practical cryptographic activity (e.g., encryptData, hashData), which is the direct transference between theory and practice. The CTF Challenge course is a group that operates the events of Capture the Challenge, which is one of the most important gamified learning features. Also, this module takes care of the third-party integration of widgets in the "Market Analysis" section, which increases the educational coverage of the platform.

8. Results

The findings indicate the successful implementation of the modules of Edu-CyberSphere, and the assessment is performed in various aspects. The performance analysis indicates that the system can support concurrent user sessions with a low latency rate and an average response time of less than 200 ms and consistent database transactions. Regarding usability, user surveys show a satisfaction rating of 4.5/5, which means that the interface is clear and the navigation is easy. The scalability of the platform is facilitated by the modular nature of the platform that can be scaled horizontally and increase in size of discussion forums and the learning tools without compromising responsiveness. Lastly, the pre- and post-tests were used to assess the effectiveness of learning, and it was discovered that the practical skills of students regarding cybersecurity increased by 25 percent since they were exposed to the integrated

cryptography tools and gamified challenges.

8.1. Secure Database and User Management Backend

The bottom-line outcome is a safe and effectively organized back-end, which would be able to work with all user and forum information. The MySQL database primary user table (xf_user) design as depicted in Fig. 2 includes key fields of authentication, user profiles and security. The fact that each user has a unique secret key generated by the system will be another security measure on top of the normal password hashing to ensure that the community has a secure and strong backend.

8.2. User Onboarding and Authentication Interface

An easy and secure registration was introduced successfully. The interface will demand the necessary user information and hCaptcha verification to eliminate automated registrations, as illustrated in Fig. 3. Moreover, it provides a simplified sign-up process through Discord, which is designed to capture the attention of the target audience of this specific platform. This outcome shows the effective execution of the adaptable and safe authentication module that was developed in the methodology.

8.3. Dynamic Community Discussion Forum

The fundamental feature of the platform, the discussion forum within the community is operational. Fig. 4 gives an example of a conversation thread, which demonstrates the intuitive user experience, the nested comments, and user profiles with the gamification features (levels and staff badges). This fact proves the effective implementation of a centralized unit of collaborative learning and communication with the user, which is the main purpose of the formation of an active online community.

8.4. Integrated Practical Learning Tools

To facilitate practical skill learning, Cryptography Ciphers module was introduced and it is entirely available to the users. The primary menu of this tool as shown in Fig. 5 offers a choice of different ciphers that can be tested by users. The outcome is a direct response to the weakness of theoretical-only learning in currently available platforms by offering a more practical and comprehensive environment to apply cryptographic concepts to, thus, increasing the acquisition of skills.

8.5. Specialized Content Modules for Expanded Learning

The content modules that were introduced into the platform helped to extend the scope of the platform beyond core subjects of cybersecurity. The dashboard of Fig. 6 is the "Market Predictions" which gives the user real-time technical analysis indicators of several assets. Also, a market capitalization tracker, which is presented in Fig. 7, provides a more global perspective of market data. The educational opportunities offered by these features are valuable and data-driven learning experiences in the field of financial technology and analysis, in contrast to the more limited educational forums.

9. Conclusion And Future Scope

9.1 Conclusion

This paper has introduced design, methodology and implementation of Edu-CyberSphere, a multidimensional education platform that was designed to overcome the constraints of

traditional e-learning forums. The incorporation of a gamified, community-based forum and practical, hands-on tools and content modules make the platform a successful means of creating an engaging and secure platform of learning cybersecurity and other new technologies. The outcomes prove the existence of a fully operational system that boosts user motivation based on gamification, offers realistic skills acquisition opportunities based on integrated cryptography and market analysis tools, and broadens the educational scope to the traditional curricula. Recent research in the area of cybersecurity education [13] confirms the efficacy of gamification in enhancing user motivation and engagement, whereas the application of secure authentication systems is consistent with the current practice to protect the data and trust the online learning environment [14]. The edu-CyberSphere proves to be a major breakthrough in cybersecurity education by combining the interactive, gamified, and secure learning in one platform. The research proves its usefulness in improving motivation, practical skills development, and interdisciplinary learning. Weaknesses are based on web-based access and the necessity of further LMS integration. The further work will concentrate on the creation of mobile applications, more profound integration of LMS, and adaptive AI-based custom learning routes to enhance the engagement and educational performance.

9.2 Future Scope

Based on the positive experience of the introduction of the specialized content modules, further improvement of the platform in terms of its interactivity and educational scope will become the subject of further work. Future development has been identified in the following areas:

1. **Advanced Data Analytics and User Interaction:** The current market analysis tools will be improved to enable increased interaction with the user. This is to be followed in the future by allowing users to execute user-provided data analysis scripts on the given market data or to upload their datasets to run them in the module, which would turn the module into a data science sandbox.

2. **Development of a Mobile Application:** In order to enhance its accessibility and user interaction, a specific iOS and Android mobile application will be created. This will give users access to the forums, learning tools and real-time notification on the go, which will further make the platform an integral part of the daily learning routin.

3. **Integration with Learning Management Systems (LMS):** In order to structure the educational journeys being provided, the platform will be combined with existing Learning Management Systems. It would enable academic institutions to make modules and challenges of Edu-Cyber Sphere part and parcel of their curriculum, and offer a smooth transition between formal learning and informal learning.

Funding Statement

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Data Availability Statement
Data sharing is not applicable to this article, as no new data was created or analyzed in this study.

Credit Authorship Contribution Statement
Author A generated the idea and drafted the first version; Author B helped to review the literature and improve the content; Author C helped to develop the methodology and structure of work; Author D helped to edit and format it; Author E helped to proofread and reference it; and Author F made significant revisions, managed the work, and is the Corresponding Author of all the journal communications. The final manuscript was accepted by all authors.

Declaration of Competing Interest
The authors declare that they have no conflict of interest.

References

[1] O. B. Adedoyin and I. Soykan, "A review of the use of online forums for learning in higher education: Benefits, challenges, and future directions," Journal of Computers in Education, vol. 8, no. 2, pp. 165–183, 2021.

[2] T. Alquraini and N. A. Abdullah, "Factors affecting e-learning acceptance among university students: A structural equation modeling approach," International Journal of Information and Communication Technology Education, vol. 8, no. 3, pp. 43–60, 2012.

[3] D. R. Garrison and T. Anderson, E-learning in the 21st century: A framework for research and practice. Routledge, 2003.

[4] L. Harasim, Online learning communities: Networks that nurture teaching and learning. Routledge, 2012.

[5] K. F. Hew and W. S. Cheung, "Students' perceptions of online forum usage: A case study of a blended learning course," British Journal of Educational Technology, vol. 45, no. 4, pp. 610–624, 2014.

[6] A. Kumar and S. Verma, "Gamification in Cybersecurity Education: A State-of-the-Art Review and Research Agenda," Journal of Applied Research in Higher Education, vol. 16, no. 3, pp. 245–268, 2024.

[7] M. Singh and R. Patel, "Enhancing Security Awareness Through Gamified Approaches," *International Journal of Smart Grid Security*, vol. 3, no. 1, pp. 88-102, 2024.

[8] J. Lee and H. Park, "SherLOCKED: A Detective-themed Serious Game for Cyber Security Education," Journal of Cybersecurity Education, Research and Practice, pp. 1–14, 2021.

[9] P. Desai and K. Sharma, "Using Gamification to Enhance Mastery of Network Security Concepts," *Journal of Cybersecurity Education, Research and Practice*, vol. 2024, no. 1, pp. 77-94, 2024.

[10] D. Pramod, “Gamification in cybersecurity education; a state of the art review and research agenda,” Journal of Applied Research in Higher Education, vol. 17, no. 4, pp. 1162–1180, Jun. 2024.

[11] W. Lazarov, T. Schafeitel-Tähtinen, J. Squillace, Z. Martinasek, A. Coufalikova, and M. Helenius, “Lessons learned from using cyber range to teach cybersecurity at different levels of education,” Technology, Knowledge and Learning, vol. 30, pp. 1–19, 2025.

[12] E. J. Lundqvist, P. S. Lillemets, and N. Dragoni, “A comparative analysis of open-source cyber ranges for cyber-security education,” Procedia Computer Science, vol. 272, pp. 415–420, 2025.

[13] R. Gupta, "Gamification in Security Awareness Training: Evidence from Higher Education," International Journal of Cybersecurity Education, vol. 5, no. 2, pp. 45–52, 2024.

[14] L. Moreno and Y. Zhao, "Secure Authentication Methods in Online Forums," International Journal of Cybersecurity Intelligence & Cybercrime, vol. 5, no. 2, pp. 112–130, 2023.