International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

DEVELOPMENT OF A CYBERSECURITY LEARNING SYSTEM WITH BUILT-IN EARNING MECHANISMS

Niranjan Shelke
Ajeenkya Dy Patil University, India

Suyog Deshmukh
(Mentor),
Ajeenkya Dy Patil University, India

Prof. Ravi Khatri
(Project Guide)
Ajeenkya Dy Patil University, India

Abstract - The rapid growth of cyber threats, including data breaches, ransomware attacks, and phishing campaigns, has significantly increased the demand for skilled cyber security professionals. However, traditional learning systems often lack hands-on practical exposure and fail to sustain user engagement over extended periods. This paper presents the design and development of a unified cyber security learning platform with integrated earning mechanisms to address these challenges.

The proposed system combines multiple features, including bug bounty programs, cyber security competitions, OSINT-based investigations, cyber esports, and interactive learning modules, within a single platform. In addition, a novel Cyber Feed module is introduced, allowing users to earn rewards while engaging with short-form cyber security content such as reels and posts, thereby transforming passive scrolling into productive learning.

Unlike conventional platforms that primarily focus on theoretical knowledge or isolated practical exercises, the proposed system provides a comprehensive environment where users can gain real-world experience while being incentivized through performance-based rewards. The platform is developed using a scalable architecture, with React.js for the frontend, Node.js and Express.js for the backend, and MySQL for data management.

Experimental observations indicate that the integration of learning and earning mechanisms significantly enhances user engagement, motivation, and skill development. The proposed approach offers a sustainable and practical solution for modern cybersecurity education and contributes to the development of a skilled cybersecurity workforce.

Keywords - Cyber security Education, Gamification, Bug Bounty, OSINT, Cyber security Training Platform, Learning Systems, Earning Mechanisms, Cyber Feed, User Engagement, Cyber Esports, Digital Learning Platforms, Skill Development

1. INTRODUCTION

The rapid advancement of digital technologies has made cyber security a major concern for individuals, organizations, and governments across the globe. With the increasing frequency of cyber threats such as phishing attacks, ransomware incidents, and data breaches, the demand for skilled cyber security professionals has grown significantly[1], [2],As cybercrime continues to evolve in complexity, it has become essential to develop effective and practical training systems that can prepare individuals for real-world challenges.

Despite this growing need, traditional cyber security education systems largely focus on theoretical concepts and often provide limited opportunities for hands-on learning [1] , [3], [4]. This creates a gap between academic knowledge and industry requirements, making it difficult for learners to acquire job-ready skills. To overcome this limitation, modern learning platforms have started incorporating practical environments and interactive approaches to enhance user learning experiences.

Several platforms have contributed to this shift. For instance, bug bounty platforms such as HackerOne and Bugcrowd allow users to discover vulnerabilities and earn rewards, encouraging ethical hacking practices [5], [6], [7]. Similarly, training platforms like TryHackMe and Hack The Box provide structured learning paths along with hands-on labs to build practical skills [5], [8]. Although these platforms are effective in their respective areas, they often focus on specific functionalities and lack a unified approach.

Gamification has emerged as a powerful method to improve user engagement and motivation in digital learning environments [9], [10]. By integrating elements such as rewards, leaderboards, and challenges, platforms can make learning more interactive and engaging. In addition, the use of Open Source Intelligence (OSINT) tools like Shodan and Maltego enables learners to perform real-world investigations, further enhancing their analytical and technical skills [11], [12].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

However, despite these advancements, there is still a lack of a comprehensive platform that integrates learning, practical exposure, and earning opportunities into a single system. Most existing solutions require users to switch between multiple platforms, which reduces efficiency and negatively impacts user engagement [13], [14].

Research Question:
"How can a unified cyber security platform effectively integrate learning, practical experience, and earning mechanisms to enhance user engagement and skill development?"

To address this challenge, this paper proposes the development of a unified cyber security learning platform that combines education, practical training, and earning opportunities within a single environment. The system integrates features such as bug bounty programs, cyber security competitions, OSINT-based challenges, cyber esports, and interactive learning modules, educational chatbots.[15] Additionally, it introduces a Cyber Feed module that enables users to earn rewards while engaging with short-form cyber security content. By bringing these elements together, the proposed platform aims to improve user engagement, enhance practical skill development, and create a sustainable ecosystem for modern cyber security education.

2. LITERATURE REVIEW

2.1 Literature Review

Digital platforms have become a major driving force in modern education by enabling scalable, flexible, and interactive learning environments [8], [16]. In the field of cyber security, several platforms and technologies have been developed to enhance skill development and provide practical exposure to learners.

Bug bounty platforms such as Hacker One and Bug crowd offer real-world environments where ethical hackers can identify vulnerabilities in systems and receive rewards for responsible disclosure [5], [17]. These platforms not only contribute to improving the security of digital systems but also provide users with valuable hands-on experience, bridging the gap between theoretical knowledge and practical application [17], [18].

Gamification has been widely recognized as an effective strategy to improve user engagement and motivation in learning systems. Research indicates that incorporating elements such as points, leaderboards, challenges, and rewards can significantly enhance learning outcomes and participation rates [3], [10]. Cyber security training platforms like TryHackMe and Hack The Box utilize gamified environments with interactive labs and scenario-based challenges, allowing users to develop practical skills in a structured manner [5], [7].

Open Source Intelligence (OSINT) tools play a critical role in modern cyber security investigations by enabling the collection and analysis of publicly available information. Tools such as Shodan, Maltego, and SpiderFoot are widely used for reconnaissance, threat analysis, and digital investigations [11], [19]. These tools enhance the analytical capabilities of users and are essential for real-world cyber security operations.

Recent advancements in artificial intelligence and machine learning have further strengthened cyber security systems. AI-driven approaches are increasingly used for threat detection, anomaly identification, and automated incident response [2], [16], [20]. These technologies improve the speed and accuracy of detecting cyber threats, making cyber security systems more efficient and adaptive to evolving attack patterns.

In addition, cyber range platforms and simulation-based training environments have been introduced to provide realistic scenarios for practicing cyber attack and defense strategies [13], [21]. These platforms allow users to gain hands-on experience in controlled environments, helping them develop problem-solving skills and practical expertise.

Despite the availability of these advanced tools and platforms, most existing solutions focus on specific aspects such as vulnerability discovery, training, or competition. There remains a lack of a unified system that integrates learning, practical experience, and earning opportunities within a single platform [3], [8], [14]. This limitation highlights the need for a comprehensive cyber security learning system that combines multiple functionalities and incorporates built-in earning mechanisms to enhance user engagement and skill development.

2.2 Motivation

The primary motivation behind this research is to address the gap between theoretical cybersecurity education and real-world practical experience. Although many learners have access to study materials and online resources, they often lack opportunities to apply their knowledge in realistic scenarios. This limitation reduces their ability to develop industry-ready skills and effectively respond to real cyber threats [4], [16].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Existing cybersecurity platforms provide valuable features such as bug bounty programs, training labs, and challenges; however, these features are typically distributed across multiple systems. As a result, users are required to switch between platforms, which reduces learning efficiency and continuity [3], [22].

Another significant factor is user engagement. Traditional learning approaches often fail to maintain user interest over long periods. Research shows that incorporating gamification elements such as rewards, competition, and interactive content can significantly improve motivation, participation, and learning outcomes [3], [10].

Furthermore, there is an increasing need to make cybersecurity education more accessible, practical, and skill-oriented. By integrating earning opportunities with learning activities, users can remain motivated while gaining hands-on experience. This combined approach forms the foundation for developing a more engaging, sustainable, and user-centric cybersecurity learning platform.

2.3 Objectives

The primary objective of this research is to design and develop a unified cybersecurity platform that integrates learning, practical experience, and competitive elements within a single system. The platform aims to provide users with real-world exposure through features such as bug bounty programs, OSINT-based investigations, and cyber security challenges, enabling them to develop practical and analytical skills [18], [19].

Another key objective is to implement a reward-based mechanism that allows users to earn incentives based on their performance and active participation. This approach is inspired by gamification models that have been proven to enhance user engagement and retention in learning environments [9].

In addition, the research focuses on improving user engagement by incorporating interactive features such as contests, cyber esports, and short-form learning content. These features are designed to create a continuous learning cycle and encourage consistent participation.

Overall, the system aims to promote cyber security awareness, improve practical skill development, and provide an accessible and scalable platform that prepares users for real-world cyber security challenges.

3. PROPOSED SYSTEM

3.1 System Overview

The proposed system, BHT-X (Bug Hunt Training & eXperience Platform), is designed as a unified cyber security platform that integrates learning, practical exposure, and earning opportunities within a single environment. Unlike existing platforms that focus on individual components such as training or bug bounty programs, the proposed system combines multiple cyber security activities to create a comprehensive and engaging ecosystem [5], [8].

The platform includes modules such as bug bounty programs, cyber security contests, OSINT-based investigations, and hands-on cyber labs.[16] These features allow users to participate in real-world scenarios where they can identify vulnerabilities, solve security challenges, and enhance their analytical and technical skills. By integrating these components, the system bridges the gap between theoretical knowledge and practical application.

A key distinguishing feature of the platform is its built-in earning mechanism. [17]Users are rewarded based on their performance, participation, and consistency across different activities such as completing challenges, reporting vulnerabilities, and engaging with learning content. This reward-based approach is inspired by gamification principles, which have been shown to significantly improve user motivation and engagement in learning systems [3], [14]. The earning system not only motivates users but also creates a sustainable learning environment where skill development is directly linked with incentives.

The platform is designed to support users with different levels of expertise, ranging from beginners to advanced learners. Structured learning paths guide new users, while advanced challenges and real-time simulations provide opportunities for experienced users to enhance their skills further.

In addition to technical modules, the system introduces interactive features such as the Cyber Feed, where users can access cyber security-related content and earn rewards through daily engagement. Another important component is Cyber Esports, which simulates team-based attack and defense scenarios, enabling users to understand real-world cyber security operations in a controlled environment [10].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Overall, the proposed system is designed with a user-friendly interface and scalable architecture, ensuring smooth navigation, accessibility, and efficient performance. By combining learning, practice, and earning in a single platform, BHT-X provides an innovative solution for modern cyber security education and skill development.

3.2 Requirements

The development and implementation of the BHT-X platform require both hardware and software resources to ensure efficient functionality and system performance. A computer system with a minimum of 8GB RAM is recommended to support development activities and handle multiple services simultaneously. Reliable internet connectivity is essential for accessing cloud-based services, APIs, and real-time platform features.

On the software side, Visual Studio Code is used as the primary development environment for coding, debugging, and project management. The backend of the system is developed using Node.js and Express.js, which provide a robust framework for handling server-side operations, API integration, and real-time communication. The frontend is implemented using React.js to create a responsive and interactive user interface that enhances user experience.

The system uses MySQL as the database management system to securely store user information, activity logs, and reward transactions. Data security measures such as input validation and secure authentication mechanisms are implemented to ensure data integrity and prevent unauthorized access [16], [17].

Furthermore, OSINT tools and APIs such as Shodan, Maltego, and SpiderFoot are integrated into the platform to support investigation-based learning and real-world data analysis [2], [19]. These integrations enhance the practical capabilities of the system and provide users with hands-on experience in cybersecurity investigations.

The platform is developed and tested on a system equipped with an Intel® Core™ i5 processor and stable network connectivity, ensuring reliable execution of backend services and user interactions. The overall system design focuses on scalability, efficiency, and seamless user experience, allowing the platform to support a large number of users and activities without performance degradation.

4. METHODOLOGY AND SYSTEM DESIGN

4.1 Methodology

The development of BHT-X follows a modular approach, where each feature such as contests, OSINT tools, and labs is developed as an independent module and later integrated into the platform. This approach improves flexibility and simplifies testing and debugging. The design is influenced by platform-based system models, where multiple services are combined into a unified ecosystem [11], [19]. The frontend is developed using React.js to provide a smooth and interactive user interface, ensuring better user experience and responsiveness. The backend is built using Node.js and Express.js to efficiently handle server-side operations, API requests, and application logic.

The database is designed using MySQL to securely store user information, contest data, and transaction records. APIs are integrated to provide additional functionalities such as OSINT data retrieval and AI-based assistance, enhancing the overall capability of the system [19], [23]. The development process follows an incremental approach, where each module is tested individually before full integration to ensure system stability.

User authentication and session management mechanisms are implemented to maintain secure access and protect sensitive data. Input validation techniques are also applied to ensure data accuracy and prevent misuse of the system. The platform supports real-time interaction between frontend and backend through efficient API communication, enabling smooth user operations. Additionally, the reward system is designed to track user activities and calculate earnings based on performance and participation, similar to gamified systems that improve user engagement [9], [10].

The overall architecture is developed with scalability in mind, allowing future enhancements such as AI-based analysis and advanced cyber security simulations to be added without affecting existing functionalities [2], [16].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The system architecture of the proposed platform is illustrated in **Fig. 1**

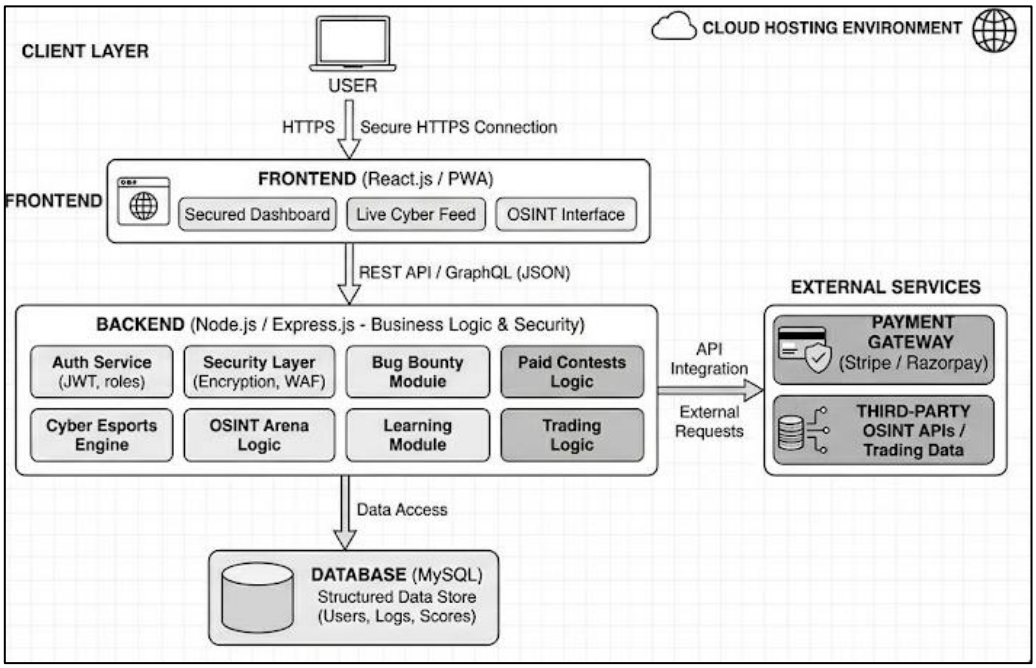

Fig. 1: System Architecture

The system architecture of BHT-X is designed using a layered approach to ensure scalability, security, and smooth communication between components. The platform begins with the client layer, where users access the system through a secure HTTPS connection using web browsers or devices.

The frontend is developed using React.js, which provides an interactive interface including dashboards, cyber feed, and OSINT features. It communicates with the backend through REST APIs and handles user interactions efficiently. " ***The frontend ensures a responsive and user-friendly experience for all platform activities***".

The backend is built using Node.js and Express.js, where the core business logic and security mechanisms are implemented. It manages modules such as authentication, bug bounty programs, contests, OSINT operations, and learning features. "***The backend acts as the central processing unit, handling all system operations and data flow***".

The system also integrates external services such as payment gateways and third-party OSINT APIs. These services support secure transactions and real-time data access. "***External integrations enhance the functionality and real-world applicability of the platform***".

All data is stored in a MySQL database, which maintains structured information such as user details, activity logs, and rewards. "***The database ensures reliable storage and efficient retrieval of system data***".

Overall, the architecture provides a secure and scalable environment that connects users, services, and data into a single unified system. "***The layered design supports seamless interaction between components while maintaining system performance and security***".

4.2 System Modules

The BHT-X platform is designed as a modular system where each component performs a specific function, ensuring efficient operation and a complete cybersecurity learning and earning environment. The system is divided into multiple interconnected modules that collectively provide practical exposure, user engagement, and administrative control. ***'A modular architecture improves scalability and allows independent development and maintenance of system components'***.

The **Authentication System** manages secure access by verifying user credentials and maintaining session control. This ensures protection of user data and prevents unauthorized access, which is a critical requirement in modern cybersecurity systems [24].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The **Programs (Bug Bounty)** module enables users to identify and report vulnerabilities in given systems. This approach promotes ethical hacking practices and reflects real-world cybersecurity workflows, contributing to better threat detection and system security [5], [18].

The **Contests** module allows users to participate in time-based cybersecurity competitions, encouraging skill development under realistic conditions. Similarly, the **Cyber Esports** module provides a simulated environment where Red Team and Blue Team activities help users understand both offensive and defensive strategies.[25] ***'Such simulation-based learning enhances practical understanding of cyber attack and defense mechanisms'***.

The **OSINT Arena** supports investigation-based tasks where users gather and analyze publicly available data. This strengthens intelligence gathering skills, which are widely used in cybersecurity analysis and threat identification[19].

The **OSINT Puzzles** module includes structured challenges such as puzzles and Capture The Flag (CTF) tasks, which improve logical thinking and analytical skills. These gamified approaches have been shown to increase engagement and learning effectiveness [11].

The **Cyber Feed** module enhances user engagement by allowing interaction with cybersecurity content. [26]Users earn rewards through participation, creating a continuous learning cycle. ***'Gamification and reward-based interaction play a significant role in maintaining user motivation'***.

The **Dark Web Challenges** module provides a controlled simulation of hidden network environments. It allows users to safely explore investigation techniques without exposure to actual risks, which is important for understanding cybercrime behavior [27].

The **Learning Module** delivers structured educational content supported by practical examples. It helps users build a strong foundation in cybersecurity concepts while also applying them in real scenarios. Modern learning systems increasingly rely on intelligent and adaptive techniques to improve training effectiveness [2], [4], [28].

Finally, the **Admin Panel** acts as the control center of the platform, enabling administrators to manage users, monitor activities, and control system operations. ***'Effective administration ensures system reliability, security, and smooth execution of all platform features'***.

The **system architecture** of the proposed platform is illustrated in **Fig. 2**

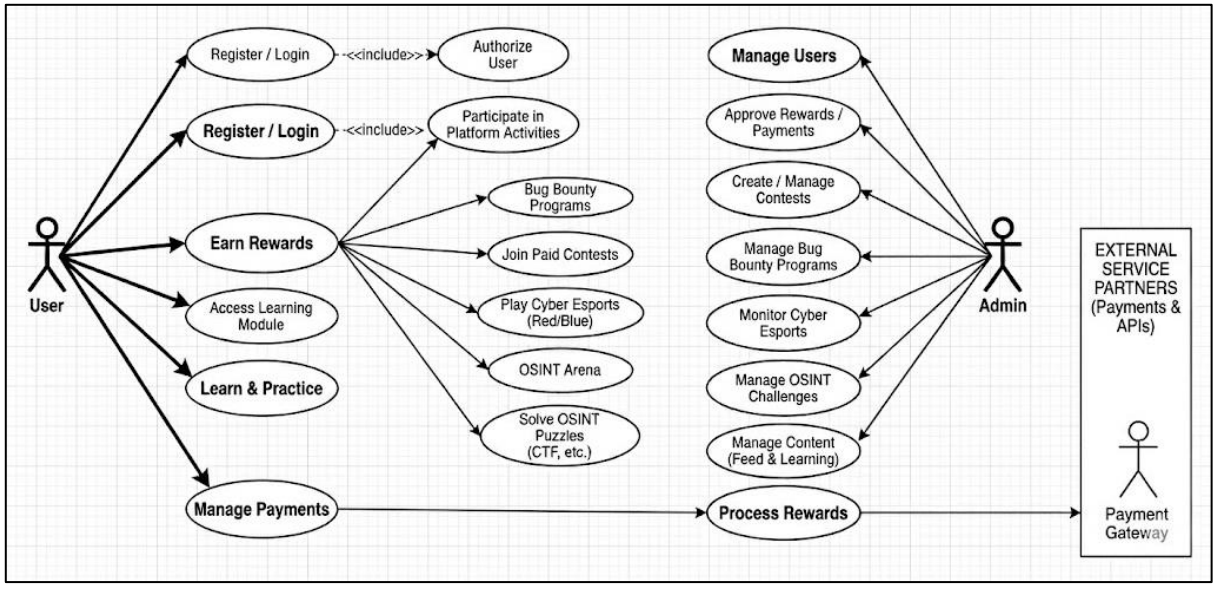

Fig. 2 Use Case Diagram

The use case diagram illustrates the interaction between the User, Admin, and the BHT-X platform. Users can register, access learning modules, participate in activities such as bug bounty programs, contests, cyber esports, and OSINT challenges, and earn rewards based on their performance. "***The system supports both learning and earning in a unified workflow***".

The Admin manages system operations, including user management, contest handling, monitoring activities, and reward processing. *The admin ensures smooth operation and control of all modules.*

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

An external payment gateway is used to handle secure transactions and reward distribution. "***External services provide secure and reliable payment processing***" .

Overall, the diagram represents how users engage with the platform while administrators maintain system functionality**.** " ***User activities are directly linked to skill development and reward generation***".

4.3 Entity Relationship (ER) Diagram

The Entity Relationship (ER) diagram of the BHT-X platform illustrates the overall data structure and defines how different entities are interconnected to manage user activities, rewards, and learning processes. The primary entity in the system is the *User*, which stores essential information such as name, email, role, and account balance. [23]The complete database design is shown in **Fig. 3**, which represents the relational structure of the system.

The *User* entity is associated with multiple modules including Programs, Contests, Cyber Esports, OSINT Arena, and Learning Modules through intermediate relational tables. [19]These relationships enable efficient tracking of user participation and performance across various activities. ***The use of relational mapping ensures accurate tracking of user interactions across the platform***.

The *Admin* entity is responsible for managing system operations such as creating programs, organizing contests, and monitoring user activities. It ensures proper control over platform functionality and content management. ***The admin plays a critical role in maintaining system integrity and smooth operation***.

Additional entities such as Payments, Submissions, Trading, and Cyber Feed are included to handle financial transactions, challenge outcomes, and user engagement. These entities are directly linked with the User entity to maintain consistency and accurate record management. ***These components support both the learning and earning aspects of the platform effectively***.

Furthermore, junction tables such as User_Programs, User_Contests, and User_OSINT are used to implement many-to-many relationships between users and platform activities.[23] ***This design enhances scalability and allows multiple users to participate in multiple modules simultaneously***.

Overall, the ER diagram provides a structured representation of the database, ensuring efficient data storage, retrieval, and management within the BHT-X platform**.** ***A well-designed database structure is essential for maintaining consistency and performance in a multi-module system***.

The ER Diagram of the proposed platform is illustrated in **Fig. 3**

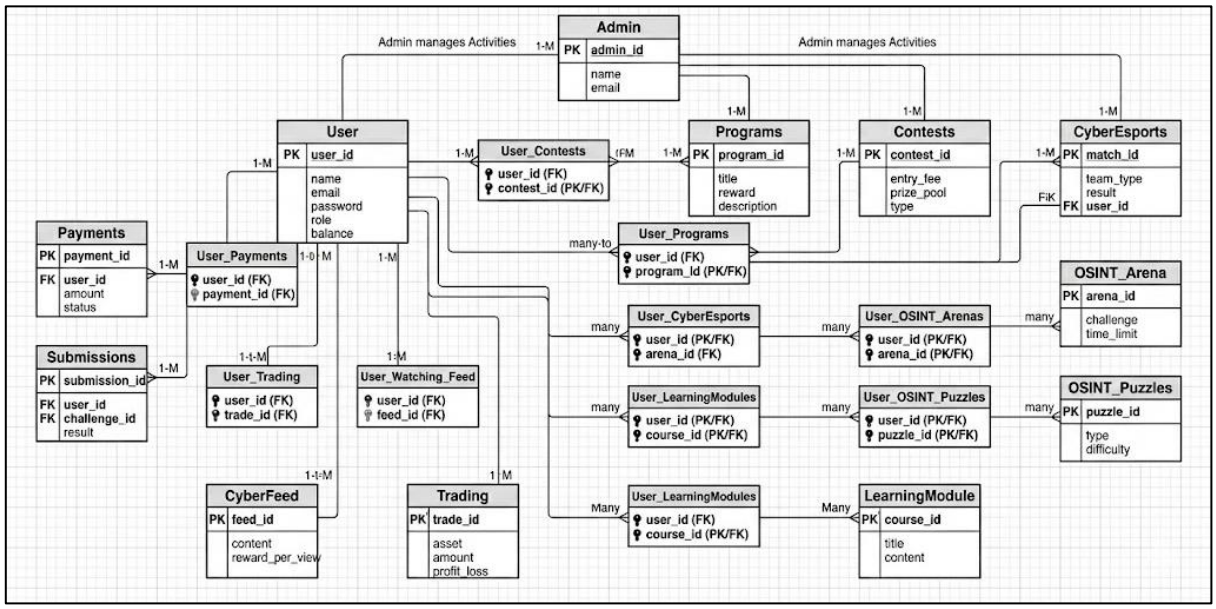

Fig. 3 ER Diagram

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

5. RESULTS & DISCUSSION

5.1 Results

The BHT-X platform was tested under multiple real-world scenarios to evaluate its performance, reliability, and usability. All system modules operated smoothly during testing without any major errors. The authentication system ensured secure user registration and login, maintaining proper session handling and data protection. Users were able to navigate the platform easily, which reflects a simple and user-friendly interface design. "***The system demonstrated stable performance even when multiple features were accessed simultaneously***".

The bug bounty module functioned effectively, allowing users to identify and submit vulnerabilities, followed by proper reward allocation. The contests module supported seamless participation, and results were accurately generated based on user performance. Similarly, the Cyber Esports module successfully simulated attack and defense scenarios, helping users experience practical cybersecurity operations. "***These modules collectively provided a real-world learning environment beyond theoretical knowledge***".

The OSINT Arena and OSINT Puzzle modules delivered time-based investigative challenges where users could apply analytical and research skills efficiently. The Cyber Feed feature also performed as expected, enabling users to earn coins through interaction with cybersecurity content such as posts and reels. ***This feature increased user engagement by combining learning with continuous rewards***.

The learning module and practical labs provided a smooth hands-on experience, allowing users to practice techniques without interruptions. The admin panel was tested for functionality such as user management, contest creation, and reward distribution, and it performed efficiently. "***Overall, the system showed consistent performance, scalability, and proper integration of all modules***".

The overall execution flow of the system, including user interaction, module processing, and reward generation, is illustrated in **Fig. 4**, which represents the workflow of the platform during operation.

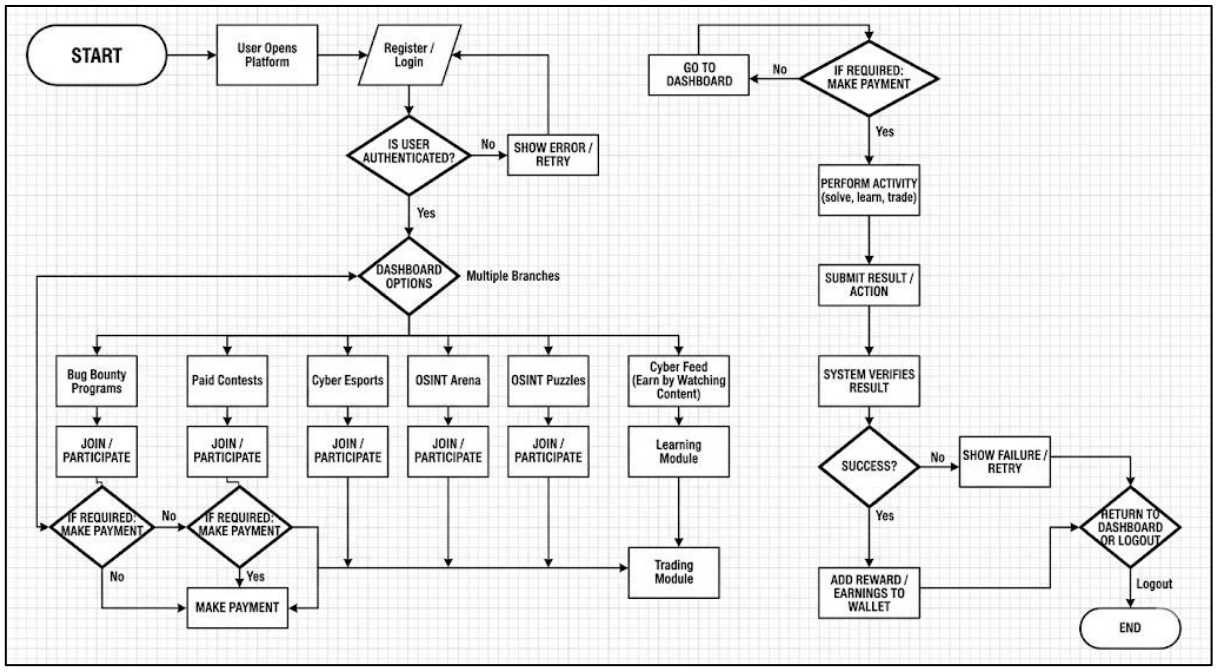

Fig. 4 System Workflow

The above flowchart represents the overall working of the BHT-X platform. The process starts when a user opens the platform and logs in. After successful authentication, the user is redirected to the dashboard where multiple features such as bug bounty programs, contests, cyber esports, and OSINT challenges are available.

"This workflow highlights how the platform integrates learning, participation, and reward mechanisms into a single system".

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Based on the selected activity, the user may be required to make a payment before participation. Once the activity is completed, the system verifies the result. If successful, rewards are credited to the user's wallet; otherwise, the user is given an option to retry. Finally, the user can return to the dashboard or log out of the system.

5.2 Discussions

The BHT-X platform demonstrates an integrated approach to cybersecurity learning by combining theoretical understanding, practical exposure, and earning opportunities within a single system.[7], [12] Unlike many existing platforms that focus either on conceptual learning or isolated competitive environments, the proposed system brings together multiple functionalities in a structured and accessible manner. "***This integration effectively reduces the gap between academic knowledge and real-world cybersecurity practice***".

The inclusion of modules such as bug bounty programs, OSINT-based challenges, and cyber esports provides users with hands-on experience that closely resembles real cybersecurity scenarios. These features allow users to apply their knowledge in practical situations, thereby improving their technical skills.[19], [22] At the same time, the reward-based mechanism encourages consistent participation and motivates users to enhance their performance. "***The earning component acts as a strong driver for user engagement, which is often lacking in traditional learning platforms***".

User engagement is further strengthened through features like the Cyber Feed and short-form cybersecurity reels, which present information in an interactive and easy-to-understand format. This approach makes learning less repetitive and helps users remain active on the platform for longer durations. "***Engagement-driven learning contributes to better retention and continuous skill development***".

The platform is designed to accommodate users with varying levels of expertise, making it suitable for both beginners and advanced learners. Its modular architecture ensures flexibility and allows the system to be extended with additional features such as AI-based recommendations, automation tools, and advanced simulation environments. ***This scalability highlights the long-term potential of the platform as a comprehensive cybersecurity ecosystem***.

Overall, the BHT-X platform offers a practical and efficient solution for modern cybersecurity education. By combining learning, real-world practice, and earning opportunities, it enhances user motivation and skill development, making it more effective compared to traditional cybersecurity learning approaches

6. CONCLUSION AND FUTURE WORK

6.1 Conclusion

The BHT-X (Bug Hunt Training & eXperience Platform) is developed as a unified cybersecurity platform that integrates learning, practical experience, and earning opportunities within a single system. The primary objective of reducing the gap between theoretical knowledge and real-world cybersecurity skills has been effectively achieved through the implementation of multiple functional modules. "***The platform successfully combines education with real-time application, making the learning process more practical and outcome-oriented***".

The system provides hands-on experience through features such as bug bounty programs, cybersecurity contests, OSINT-based investigations, cyber esports, and interactive labs. These components enable users to understand real-world scenarios and enhance their technical capabilities. In addition, the reward-based mechanism encourages continuous participation and motivates users to improve their performance over time. The integration of earning with learning creates a strong incentive for consistent engagement.

The inclusion of the Cyber Feed further improves user interaction by delivering short-form cyber security content along with daily earning opportunities.[29] The platform is designed with a user-friendly interface, making it accessible to both beginners and advanced users. ' ***Overall, the proposed system demonstrates a scalable and effective approach to modern cyber security education and skill development'***. Furthermore, the platform lays a strong foundation for developing industry-ready professionals by combining theoretical understanding with practical exposure.

6.2 Future Work

The BHT-X platform offers several opportunities for future enhancements to further improve its functionality and impact. One of the key areas of development includes the integration of AI-based personalized learning systems and intelligent chatbots, which can provide real-time guidance and adaptive learning experiences.[30] Additionally, advanced cyber attack simulation environments can be introduced to replicate complex real-world scenarios more accurately. These improvements can significantly enhance the depth and effectiveness of practical training.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The development of a mobile application can increase accessibility and allow users to interact with the platform more conveniently. Future updates may also include live mentoring sessions, certification programs, and collaborations with cybersecurity organizations to provide real industry exposure.[31] Furthermore, new earning features, an improved user interface, and increased automation can enhance user engagement and platform efficiency. Continuous innovation in these areas will help maintain long-term user interest and platform growth.

The development of more earning modules in platform , that users can earn daily and make huge profit, Enhancing the reward system with secure and transparent payment mechanisms, along with expanding OSINT tools and lab environments, will further strengthen the platform. In addition, incorporating real-time analytics and performance tracking can help users monitor their progress and improve their skills effectively. "***With these advancements, BHT-X has the potential to evolve into a comprehensive and industry-recognized cyber security ecosystem***".

REFERENCES

[1] R. A. Nafea and M. Amin Almaiah, "Cyber Security Threats in Cloud: Literature Review," in *2021 International Conference on Information Technology (ICIT)*, Amman, Jordan: IEEE, Jul. 2021, pp. 779–786. doi: 10.1109/ICIT52682.2021.9491638.

[2] G. Apruzzese *et al.*, "The Role of Machine Learning in Cybersecurity," *Digital Threats*, vol. 4, no. 1, pp. 1–38, Mar. 2023, doi: 10.1145/3545574.

[3] K. Boopathi, S. Sreejith, and A. Bithin, "Learning Cyber Security Through Gamification," *Indian Journal of Science and Technology*, vol. 8, no. 7, p. 642, Apr. 2015, doi: 10.17485/ijst/2015/v8i7/67760.

[4] A. Vaish, R. Kumar, S. Bobek, and S. Sternad, "Development of Cyber Security Platform for Experiential Learning," *Journal of Cybersecurity Education, Research and Practice*, vol. 2024, no. 1, Jun. 2024, doi: 10.62915/2472-2707.1184.

[5] J. Arshad, M. Talha, B. Saleem, Z. Shah, H. Zaman, and Z. Muhammad, "A Survey of Bug Bounty Programs in Strengthening Cybersecurity and Privacy in the Blockchain Industry," *Blockchains*, vol. 2, no. 3, pp. 195–216, Jul. 2024, doi: 10.3390/blockchains2030010.

[6] S. Alnutefy, "Effectiveness of Bug Bounty Programs in Strengthening Cybersecurity".

[7] K. Sridhar and M. Ng, "Hacking for good: Leveraging HackerOne data to develop an economic model of Bug Bounties," *Journal of Cybersecurity*, vol. 7, no. 1, p. tyab007, Feb. 2021, doi: 10.1093/cybsec/tyab007.

[8] G. Hatzivasilis *et al.*, "Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees," *Applied Sciences*, vol. 10, no. 16, p. 5702, Aug. 2020, doi: 10.3390/app10165702.

[9] MKSSS'S Cummins College of Engineering for women, Pune, Maharashtra, India, S. Thombre, M. Velankar, and MKSSS'S Cummins College of Engineering for women, Pune, Maharashtra, India, "Gamification by Students: An effective approach to cyber security concept learning," *JEET*, vol. 36, no. S1, pp. 73–81, Dec. 2022, doi: 10.16920/jeet/2022/v36is1/22178.

[10] A. Kevin Gwenhure and S. Nam, "Gamified Cybersecurity Initiatives: The Trend, Limits and Lessons," *JITE:Research*, vol. 24, p. 024, 2025, doi: 10.28945/5601.

[11] D. Govardhan, G. G. S. H. Krishna, V. Charan, S. V. A. Sai, and R. R. Chintala, "Key Challenges and Limitations of the OSINT Framework in the Context of Cybersecurity," in *2023 2nd International Conference on Edge Computing and Applications (ICECAA)*, Namakkal, India: IEEE, Jul. 2023, pp. 236–243. doi: 10.1109/ICECAA58104.2023.10212168.

[12] О. Буров, О. Бутнік-Сіверський, О. Орлюк, and К. Горська, "CYBERSECURITY AND INNOVATIVE DIGITAL EDUCATIONAL ENVIRONMENT," *ITLT*, vol. 80, no. 6, pp. 414–430, Dec. 2020, doi: 10.33407/itlt.v80i6.4159.

[13] R. Toth and L. Erd, "Expanding Horizons: The Evolving Landscape of Development Opportunities in Cybersecurity Training Platforms".

[14] P. Pornpongtechavanich and P. Wannapiroon, "Intelligent Interactive Learning Platform for Seamless Learning Ecosystem to Enhance Digital Citizenship's Lifelong Learning," *Int. J. Emerg. Technol. Learn.*, vol. 16, no. 14, p. 232, Jul. 2021, doi: 10.3991/ijet.v16i14.22675.

[15] K. Mageira, D. Pittou, A. Papasalouros, K. Kotis, P. Zangogianni, and A. Daradoumis, "Educational AI Chatbots for Content and Language Integrated Learning," *Applied Sciences*, vol. 12, no. 7, p. 3239, Mar. 2022, doi: 10.3390/app12073239.

[16] G. Kinayat, N. Kurbanali, O. Sadan, N. Kavkayeva, A. Seisagatova, and K. Abisheva, "Analysis of Cybersecurity EducationPrograms for Undergraduate Students: Review," *JETC*, vol. 4, no. 1, Mar. 2026, doi: 10.47344/8svzw234.

[17] E. Bates, V. Mavroudis, and C. Hicks, "Reward Shaping for Happier Autonomous Cyber Security Agents," in *Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security*, Copenhagen Denmark: ACM, Nov. 2023, pp. 221–232. doi: 10.1145/3605764.3623916.

[18] S. Alnutefy, "Effectiveness of Bug Bounty Programs in Strengthening Cybersecurity".

[19] Z. Avrahami, M. Zwilling, and C. Hajaj, "Leveraging OSINT for Advanced Proactive Cybersecurity: Strategies and Solutions," *IEEE Access*, vol. 13, pp. 154229–154250, 2025, doi: 10.1109/ACCESS.2025.3603868.

[20] M. A. Ferrag, L. Maglaras, H. Janicke, and R. Smith, "Deep Learning Techniques for Cyber Security Intrusion Detection : A Detailed Analysis," presented at the 6th International Symposium for ICS & SCADA Cyber Security Research 2019, 2019. doi: 10.14236/ewic/icscsr19.16.

[21] 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, doi: 10.1109/ACCESS.2021.3093952.

[22] F. Chukwuma, "USERS' BEHAVIOR AND DECISION MAKING IN CYBERSECURITY CONTEXT.," . *Vol*, vol. 1, no. 2.

[23] B. A, "Evaluating Database Security and Cyber Attacks: A Relational Approach," *J Internet Bank Commer*, vol. 20, no. 2, 2015, doi: 10.4172/1204-5357.1000115.

[24] M. A. Hossain, Md. A. Raza, and J. Y. Rahman, "Investigating the Cybersecurity Implications of Open Banking and Application Programming Interfaces (APIs) in the Financial Sector," *MINISTAL*, vol. 4, no. 1, pp. 39–56, Jan. 2025, doi: 10.55927/ministal.v4i1.13370.

[25] D. Getty, H. Li, M. Yano, C. Gao, and A. E. Hosoi, "Luck and the Law: Quantifying Chance in Fantasy Sports and Other Contests," *SIAM Rev.*, vol. 60, no. 4, pp. 869–887, Jan. 2018, doi: 10.1137/16M1102094.

[26] Temitayo Oluwaseun Abrahams, Oluwatoyin Ajoke Farayola, Simon Kaggwa, Prisca Ugomma Uwaoma, Azeez Olanipekun Hassan, and Samuel Onimisi Dawodu, "CYBERSECURITY AWARENESS AND EDUCATION PROGRAMS: A REVIEW OF EMPLOYEE ENGAGEMENT AND ACCOUNTABILITY," *Comput. sci. IT res. j.*, vol. 5, no. 1, pp. 100–119, Jan. 2024, doi: 10.51594/csitrj.v5i1.708.

[27] M. Chertoff and T. Simon, "The Impact of the Dark Web on Internet Governance and Cyber Security".

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

[28] I. H. Sarker, “Multi-aspects AI -based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview,” *Security and Privacy*, vol. 6, no. 5, p. e295, Sep. 2023, doi: 10.1002/spy2.295.
[29] E. Oat, “Integrating payment solutions to online marketplaces”.
[30] H. Szmurlo and Z. Akhtar, “Digital Sentinels and Antagonists: The Dual Nature of Chatbots in Cybersecurity,” *Information*, vol. 15, no. 8, p. 443, Jul. 2024, doi: 10.3390/info15080443.
[31] J. Kim and J. Yoo, “Platform Growth Model: The Four Stages of Growth Model,” *Sustainability*, vol. 11, no. 20, p. 5562, Oct. 2019, doi: 10.3390/su11205562.