AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
E-ISSN: 3069-0110
Vol.4, No. 4(2025)
www.ajmimc.com

CYBER KIDS-VIDEO GAME FOR RAISING CYBER SECURITY AWARENESS IN CHILDREN

Dr V Shiva Narayana Reddy[1], Paneti Rahul[2], Samanthula Geetha[3], Golla Rakesh[4], Sheelam Sujith Reddy[5] and Akella Subrahmanya Sai Anil[6]

[1]*Associate Professor, Department of CSE, Samskruti College Of Engineering And Technology, Kondapur (V), Ghatkesar (M), Medchal (D), Hyderabad, India.*

[2,3,4,5,6]*Student, Department of CSE, Samskruti College Of Engineering And Technology, Kondapur (V), Ghatkesar (M), Medchal (D), Hyderabad, India.*

Corresponding email ID: vsn.reddy5017@gmail.com

ABSTRACT:

To provide ubiquitous access, scalability and sharing possibilities, the Industrial Internet of Things (IIoT) applications utilize the cloud to store collected data streams. However, secure storing and sharing of the massive and continuously generated data poses significant privacy risks, including data breaches. This paper proposes SmartCrypt, a data storing and sharing system that supports analytics over the encrypted time series data. SmartCrypt enables users to secure and fine grain sharing of their encrypted data using a novel symmetric homomorphic encryption scheme. Simulation results show that SmartCrypt reduces query time by 17% and improves throughput by 9% over the benchmark scheme.

1 INTRODUCTION

In smart manufacturing, Industrial Internet of Things (IIoT) devices produce a significant amount of time series data related to production, monitoring and maintenance that need to be processed and stored. Due to storage and processing constraints of IIoT devices, nowadays the data storage and processing functionalities are mostly shifted to the time series database in cloud platform, e.g., Azure Time Series Insight. Further, processing and storing the data in the cloud platform enhances ubiquitous access, scalability and sharing possibilities. However, secure data storing in the cloud poses significant privacy risks, including unauthorized access of production line efficiency data. To address privacy risks, encrypted databases have appeared as a promising solution.

The main advantage of this approach is that it allows data owners and third-party services to query encrypted data while maintaining both functionality and confidentiality. Recently, research in this domain has led to several encrypted databases, e.g., relational databases and batch analytics.

Secure time series data storing in the cloud and sharing them with third-party services come with unique performance and challenges that current encrypted data processing systems fail to meet.

To address these challenges, numerous databases have been devised, particularly for time series data. However, all these databases incur significant overhead during encrypted data processing. Besides, another key challenge in smart manufacturing is that privacy should co-exist during queries on data statistics, e.g., finding the standard deviation, which usually indicates sharing data to be examined by third-party services. Further, data sharing must be fine grained as it is often unnecessary to provide third-parties free access to the data.

Instead, data owners might like to (i) share only statistical computation of the data, e.g., mean, sum, max, min, (ii) restrict the granularity at which such statistical computations are reported, e.g., per-minute, perhour, (iii) restrict the time interval over which queries are generated, e.g., February 2021, and (iv) a combination of earlier three choices. We believe that support for encrypted query processing should go together with access control to restrict the scope of data that users may query. The sharing procedure for data stream stored in the time series databases is considerably distinct from traditional databases. Particularly, in smart manufacturing, various

Received: 20-09-2025 | Accepted: 24-10-2025 | Published: 31-10-2025 |

levels of production process continuously push data streams to the cloud, where numerous services can subscribe to access and analyze data streams. Furthermore, often there is a requirement to aggregate and analyze time series data from different production processes collaboratively.

This indicates that we require to design an end-to-end encryption technique that is compatible with this sharing procedure. Most of the existing state-of-the-art security solutions are designed for relational databases instead of time series database . Although, the researchers in have proposed a security mechanism for storing and sharing of data streams, it is vulnerable to the malleability attacks. Besides, the existing time series databases failed to provide suitable access policies to allow data owners a fine-grain protection during selective and secure sharing of data streams with third-party services in multi-user smart manufacturing settings. Our main contributions in this paper are three fold.

- We design SmartCrypt, a symmetric homomorphic encryption-based access control technique for flexible and fine-grain sharing of encrypted data streams.
- We introduce a Homomorphic Message Authentication Code (HomMAC) based verification technique that supports source authentication and provides data integrity checks.
- Our experimental results show that SmartCrypt significantly improves the query time, latency and throughput compared to the state-of-the-art realization, TimeCrypt.

2 LITERATURE SURVEY

Today, enterprises collect large amounts of data and leverage the cloud to perform analytics over this data. Since the data is often sensitive, enterprises would prefer to keep it confidential and to hide it even from the cloud operator. Systems such as CryptDB and Monomi can accomplish this by operating mostly on encrypted data; however, these systems rely on expensive cryptographic techniques that limit performance in true “big data” scenarios that involve terabytes of data or more.

This paper presents Seabed, a system that enables efficient analytics over large encrypted datasets. In contrast to previous systems, which rely on asymmetric encryption schemes, Seabed uses a novel, additively symmetric homomorphic encryption scheme (ASHE) to perform large-scale aggregations efficiently. Additionally, Seabed introduces a novel randomized encryption scheme called Splayed ASHE, or SPLASHE, that can, in certain cases, prevent frequency attacks based on auxiliary data.

The recent great technological advance has led to a broad proliferation of Monitoring Infrastructures, which typically keep track of specific assets along time, ranging from factory machinery, device location, or even people. Gathering this data has become crucial for a wide number of applications, like exploration dashboards or Machine Learning techniques, such as Anomaly Detection. Time-Series Databases, designed to handle these data, grew in popularity, becoming the fastest-growing database type from 2019. In consequence, keeping track and mastering those rapidly evolving technologies became increasingly difficult. This paper introduces the holistic design approach followed for building NagareDB, a Time-Series database built on top of MongoDB—the most popular NoSQL Database, typically discouraged in the Time-Series scenario. The goal of NagareDB is to ease the access to three of the essential resources needed to building time-dependent systems: Hardware, since it is able to work in commodity machines; Software, as it is built on top of an open-source solution; and Expert Personnel, as its foundation database is considered the most popular NoSQL DB, lowering its learning curve. Concretely, NagareDB is able to outperform MongoDB recommended implementation up to 4.7 times, when retrieving data, while also offering a stream-ingestion up to 35% faster than InfluxDB, the most popular Time-Series database. Moreover, by relaxing some requirements, NagareDB is able to reduce the

Received: 20-09-2025 | Accepted: 24-10-2025 | Published: 31-10-2025 |

disk space usage up to 40%.

Data owners outsource their databases into the cloud to enjoy the quality services provided by the cloud service providers. However, using cloud database makes the private data vulnerable and exposed to the attackers including malicious insiders. Many researchers try to find the way to encrypt the cloud database and execute queries securely on the ciphertext. In this paper, we propose a secure and highly available cloud database system in the multi-cloud named SHAMC. Specifically, we use the idea of secure multiparty computation and homomorphic encryption to store data and execute queries direct on the ciphertext. Besides, the entire database is stored in multiple clouds to avoid service interruption as well as solve the problems of permanent failure and vendor lock-in. We implement the prototype of SHAMC which supports all queries in TPC Benchmark™ H (TPC-H) on the top of the commercial cloud. SHAMC is proved to be highly available and cost-efficient. The evaluation shows it has an acceptable query overhead which is superior to other encrypted cloud databases.

3 SYSTEM ANALYSIS

3.1 EXISTINGSYSTEM

The current landscape for cybersecurity awareness in children lacks a comprehensive and engaging platform. Existing approaches often rely on conventional educational methods that may not fully capture the attention of the younger audience. Limited interactive and immersive experiences contribute to a potential gap in understanding essential cybersecurity principles among children. Moreover, the absence of dedicated video games specifically designed for raising cybersecurity awareness further underscores the need for a novel and effective solution. In this context, the "CyberKids" project seeks to address these shortcomings by introducing an innovative video game that not only captures the interest of children but also imparts crucial cybersecurity knowledge in a fun and interactive manner.

DISADVANTAGES:

1. Age Group Specificity: The game's effectiveness might be limited by its focus on a specific age group. Tailoring content to a particular age range could inadvertently exclude older or younger children, potentially leaving a portion of the target audience without adequate cybersecurity education.
2. Technology Access: The success of the project relies on children having access to the necessary technology, such as computers, tablets, or gaming consoles. Economic disparities or limited access to these devices might hinder the reach of the game, particularly in underserved communities.
3. Learning Style Variability: Children have diverse learning styles, and while a video game format may resonate with many, it might not suit every child's preferred learning method. Some children may benefit more from alternative educational approaches, and the game's impact could be limited in reaching those with different learning preferences.
4. Limited Offline Engagement: The game's dependence on digital devices could limit its accessibility in offline environments. Children without consistent internet access or those in areas with poor connectivity might miss out on the educational benefits offered by the game, restricting its reach to specific demographics.
5. Content Evolution: Given the rapidly changing nature of technology and cybersecurity threats, there's a risk that the game's content might become outdated over time. Regular updates and maintenance are crucial to ensure that the information presented remains relevant and aligned with the evolving landscape of cybersecurity.

3.2 PROPOSEDSYSTEM

The "CyberKids" project aims to overcome the limitations of existing cybersecurity awareness initiatives by

Received: 20-09-2025 | Accepted: 24-10-2025 | Published: 31-10-2025 |

introducing a dynamic and interactive video game designed to engage children of various age groups. The proposed system incorporates several innovative features to enhance its educational impact:

Adaptive Learning Modules: The game will employ adaptive learning algorithms to tailor content based on individual progress and understanding. This ensures that children with different learning speeds and styles can benefit from a personalized and effective educational experience.

Multi-Platform Accessibility: Recognizing the diversity of technology access, the proposed system will be designed to run on multiple platforms, including computers, tablets, and mobile devices. This approach aims to reach a broader audience, including those with varying levels of access to digital devices.

Offline Engagement: To address concerns related to internet connectivity, the game will feature offline modes, allowing children to access educational content even in environments with limited or no internet access. This inclusivity ensures that the benefits of the game are accessible to a wider demographic.

Continuous Content Updates: To counteract the dynamic nature of cybersecurity threats, the proposed system will implement a content update system. Regular updates will introduce new challenges, scenarios, and information, keeping the game's content relevant and aligned with the ever-evolving landscape of cybersecurity.

Incorporation of Gamification Elements: Leveraging the power of gamification, the system will introduce engaging challenges, rewards, and interactive storytelling to make learning about cybersecurity not only informative but also entertaining. This approach aims to captivate children's interest and sustain their engagement over time.

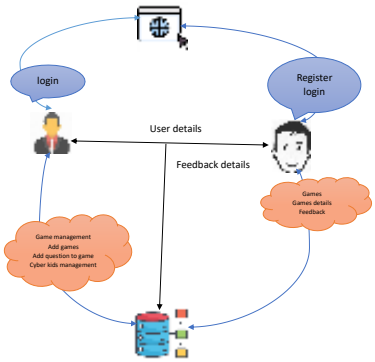
ADVANTAGES:

- Engaging and Interactive Learning: The video game format provides a highly engaging and interactive learning experience for children. By integrating educational content seamlessly into a captivating game environment, the project encourages active participation and sustains children's interest in cybersecurity concepts.
- Personalized Learning Experience: The proposed system incorporates adaptive learning algorithms to tailor content based on individual progress and understanding. This personalization ensures that each child receives a customized learning experience, accommodating different learning styles and paces.
- Multi-Platform Accessibility: Designed to run on various platforms such as computers, tablets, and mobile devices, the project ensures accessibility to a broad audience. This multi-platform approach allows children with diverse technology access to benefit from the educational content, promoting inclusivity.
- Offline Access for Wider Reach: The inclusion of offline modes in the game addresses concerns related to internet connectivity. This feature enables children in areas with limited or no internet access to still engage with the educational content, expanding the reach of the project to underserved communities.
- Continuous Learning and Updates: The proposed system's content update mechanism ensures that the game remains relevant in the face of evolving cybersecurity threats. Regular updates introduce new challenges, scenarios, and information, fostering a continuous learning experience and keeping children informed about the latest developments in the field.

Received: 20-09-2025 | Accepted: 24-10-2025 | Published: 31-10-2025 |

4 SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE



4.2 UML DIAGRAM'S:

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.

The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems.

The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems.

The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

GOALS:

The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.
4. Provide a formal basis for understanding the modeling language.
5. Encourage the growth of OO tools market.
6. Support higher level development concepts such as collaborations, frameworks, patterns and components.
7. Integrate best practices.

USE CASE DIAGRAM:

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

5 IMPLEMENTATION

5.1 MODULES:

1. USER

5.2 MODULE DESCRIPTION

Cybersecurity Basics Module: This foundational module introduces children to essential concepts of cybersecurity, such as the importance of strong passwords, recognizing phishing attempts, and understanding the basics of online safety. It serves as a starting point for building their awareness of potential online threats.

Interactive Scenario Challenges: This module presents children with realistic, interactive scenarios where they must apply cybersecurity knowledge to make decisions and solve problems. These challenges simulate real-world situations, allowing children to practice and reinforce their understanding of cybersecurity principles in a safe virtual environment.

Gamified Learning Paths: Implementing gamification elements, this module offers a structured learning path with levels, achievements, and rewards. Children progress

Received: 20-09-2025 | Accepted: 24-10-2025 | Published: 31-10-2025 |

through the game by completing educational challenges, earning points, and unlocking new content. This approach not only motivates continuous engagement but also tracks individual progress.

Offline Learning Adventures: To accommodate varying internet access, an offline module provides educational content that can be accessed without an internet connection. This feature ensures that children in areas with limited connectivity can still benefit from the game, promoting inclusivity and widening the reach of cybersecurity education.

Cybersecurity Team Challenges: Fostering collaborative learning, this module allows children to team up with virtual characters or other players to tackle cybersecurity challenges together. By promoting teamwork and communication, this module enhances social aspects of the learning experience and reinforces the importance of collective cybersecurity responsibility

Code:

```
BEGIN

  DISPLAY "Welcome to the Game Management System"

  // --- USER REGISTRATION & LOGIN SECTION ---
  PROMPT "Are you a registered user? (yes/no): "
  IF response == "no" THEN
    CALL RegisterUser()
  ENDIF

  CALL Login()

  // --- ROLE VERIFICATION ---
  IF user_role == "Admin" THEN
    CALL AdminDashboard()
  ELSE IF user_role == "User" THEN
    CALL UserDashboard()
  ELSE
    DISPLAY "Invalid role. Access denied."
  ENDIF

END


// ---------------------------
// FUNCTION DEFINITIONS
// ---------------------------

FUNCTION RegisterUser()
  DISPLAY "Enter username, password, email"
  INPUT username, password, email
  STORE user_details IN Database
  DISPLAY "Registration successful. Please login."
END FUNCTION


FUNCTION Login()
  DISPLAY "Enter username and password"
  INPUT username, password
  VALIDATE credentials WITH Database

  IF valid == TRUE THEN
    SET user_role = GET role FROM Database
    DISPLAY "Login successful as " + user_role
  ELSE
    DISPLAY "Invalid credentials. Try again."
    CALL Login()
  ENDIF
END FUNCTION


// ---------------------------
// USER OPERATIONS
// ---------------------------
FUNCTION UserDashboard()
  DISPLAY "1. View Games"
  DISPLAY "2. View Game Details"
  DISPLAY "3. Submit Feedback"
  DISPLAY "4. Logout"

  INPUT choice

  SWITCH(choice)
    CASE 1:
      CALL ViewGames()
    CASE 2:
```

Received: 20-09-2025 | Accepted: 24-10-2025 | Published: 31-10-2025 |

```
        CALL ViewGameDetails()
      CASE 3:
        CALL SubmitFeedback()
      CASE 4:
        DISPLAY "Logged out successfully."
      DEFAULT:
        DISPLAY "Invalid choice."
    END SWITCH
END FUNCTION


FUNCTION ViewGames()
    FETCH games_list FROM Database
    DISPLAY games_list
END FUNCTION
```

```
FUNCTION ViewGameDetails()
    PROMPT "Enter Game ID:"
    INPU
```

6 RESULTS/DISCUSSION

6.1 SYSTEM TEST

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

TESTCASES

Testcase1forLoginform:

FUNCTION:	**LOGIN**
EXPECTEDRESULTS:	ShouldValidatetheuserandcheckhis existence in database
ACTUAL RESULTS:	Validatetheuserandcheckingtheuser against the database
LOW PRIORITY	**No**
HIGH PRIORITY	**Yes**

Testcase2:

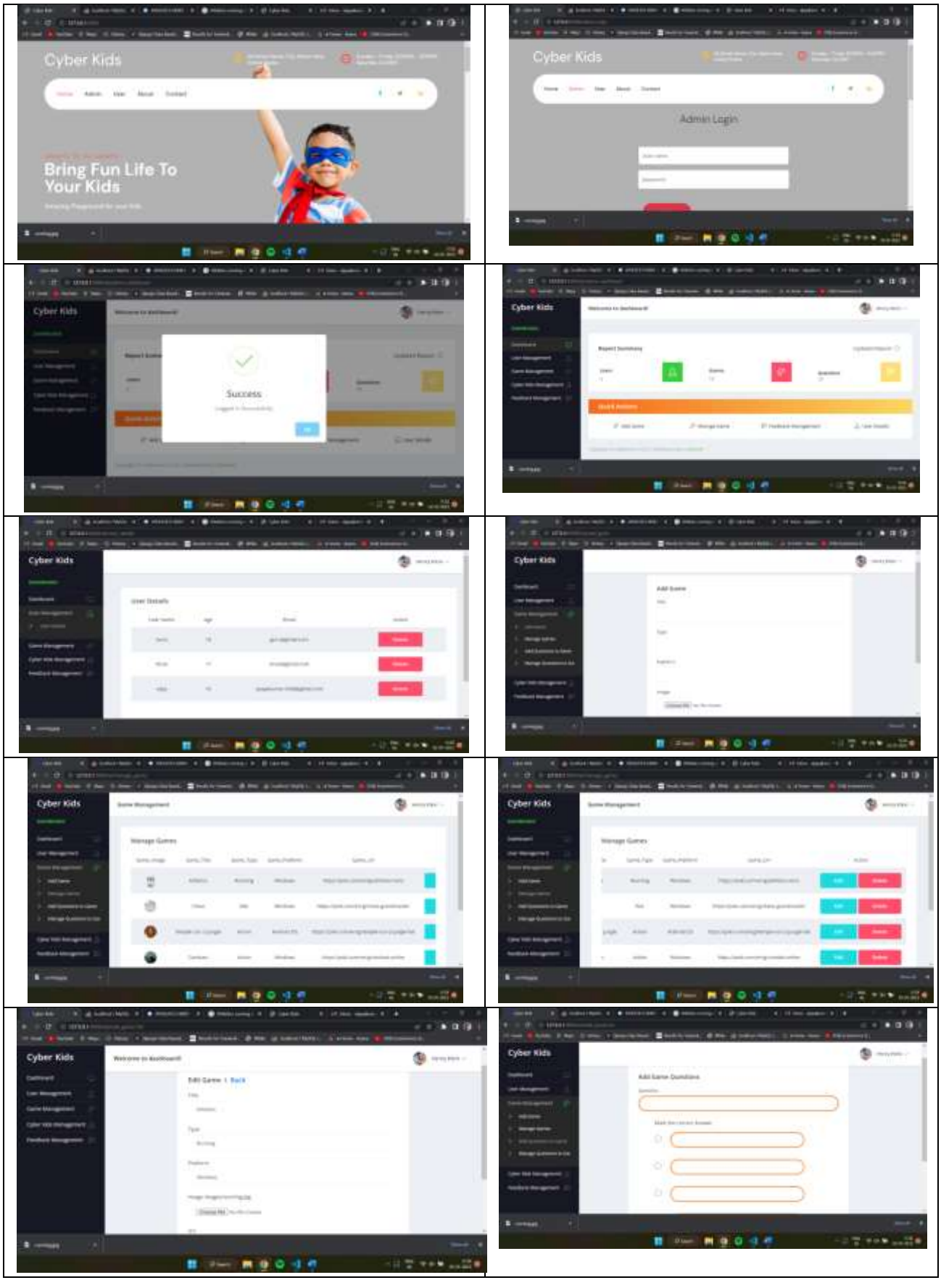
TestcaseforUserRegistrationform:

FUNCTION	USERREGISTRATION
EXPECTEDRESULTS:	Shouldcheckifallthe fields arefilledby the userandsavingthe userto database.
ACTUALRESULTS:	Checkingwhetherallthe fields arefilledby userornotthroughvalidationsandsaving user.
LOWPRIORITY	No
HIGHPRIORITY	Yes

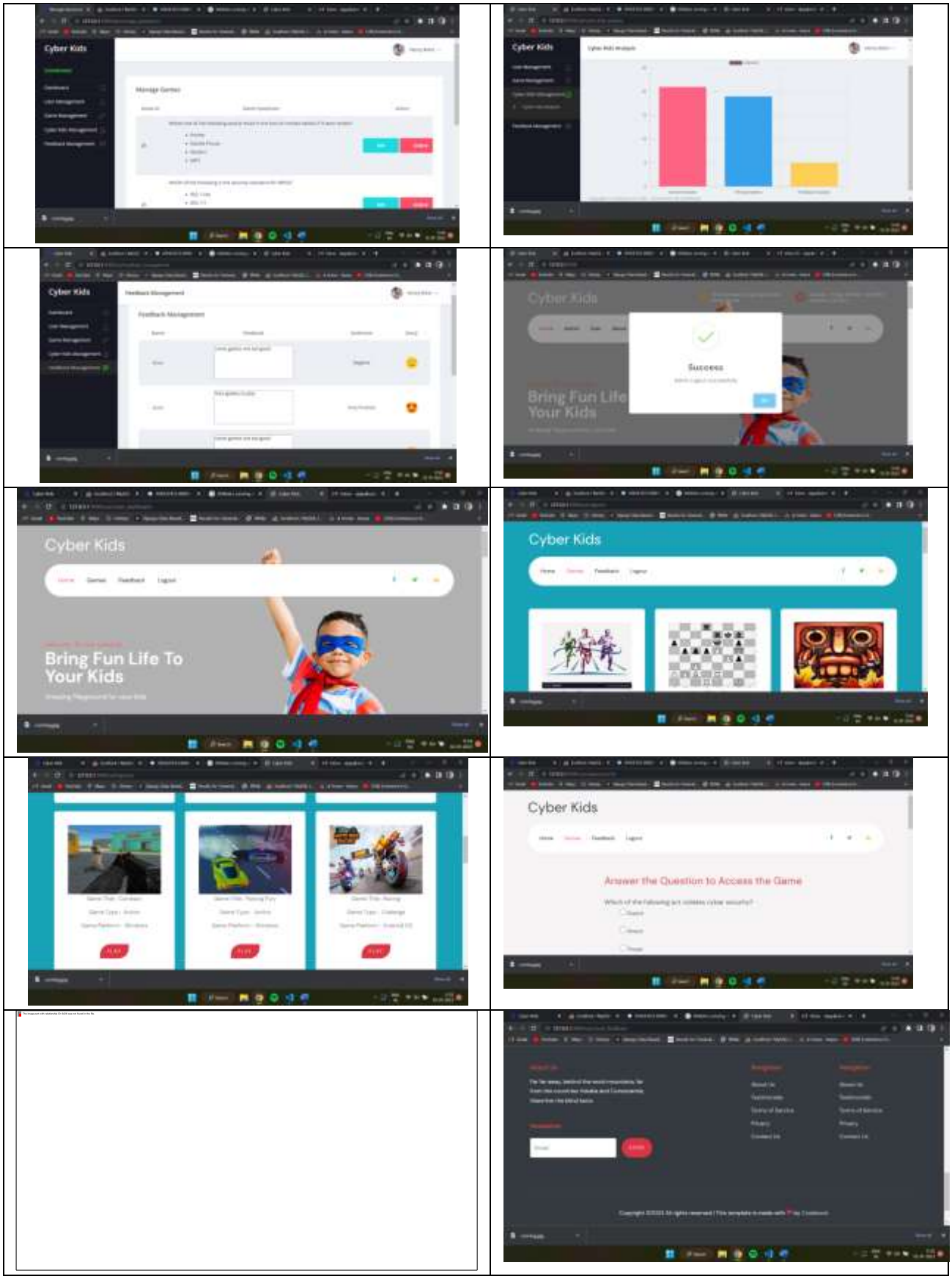
Received: 20-09-2025 | Accepted: 24-10-2025 | Published: 31-10-2025 |

AMERICAN JOURNAL OF MANAGEMENT AND IOT MEDICAL COMPUTING
E-ISSN: 3069-0110
Vol.4, No. 4(2025)
www.ajmimc.com

SCREENSHOTS



Received: 20-09-2025 | Accepted: 24-10-2025 | Published: 31-10-2025 |



7 CONCLUSION

This article elaborates on the detection method of whether to wear a helmet based on YOLOv5s, including the processing process of YOLOv5s, data set processing, training and model optimization. The experimental results

show that the model has achieved good results in test accuracy and detection speed. Evaluated on our 1574 test set, the model achieves an accuracy of 91.8%. In the environment without GPU, the average detection speed reached 35fps. However, the helmet detection model based on YOLOv5s will miss detection on overlapping targets. The next step is improving the network structure for overlapping scenes and increasing the diversity of training samples. To improve the quality of training samples, in-depth exploration is needed in the future.

FUTURE SCOPE

Growing Demand for Cybersecurity Education:

Increasing Cyber Threats: As cyber threats continue to evolve, there is a rising need to educate younger generations about safe online behavior.

Curriculum Integration: Schools and educational institutions are likely to integrate digital literacy and cybersecurity education into their curricula, creating a demand for educational tools like "Cyber Kids."

Market Potential:

- Educational Technology (EdTech) Growth: The EdTech market is expanding rapidly, offering a significant opportunity for educational games.
- Parental Interest: Parents are becoming more aware of online safety issues and are likely to support games that educate their children on these topics.

Technology Advancements:

- Interactive and Immersive Experiences: Advances in gaming technology, such as virtual reality (VR) and augmented reality (AR), can enhance the learning experience, making it more engaging and effective.
- AI and Personalization: Artificial intelligence can be used to tailor the game experience to individual learning styles and paces, improving educational outcomes.

Collaboration Opportunities:

- Partnerships with Schools and Educators: Collaborating with educational institutions can help in aligning the game with educational standards and enhancing its credibility.
- Corporate Sponsorships and Partnerships: Companies focused on cybersecurity may sponsor or partner with the game to promote online safety, providing financial support and expertise.

Global Reach:

- Multilingual Support: Developing the game in multiple languages can increase its accessibility and reach a global audience, spreading awareness on a larger scale.
- Cultural Adaptation: Tailoring the game content to different cultures can make it more relevant and impactful across various regions.

REFERENCES

1. A. Papadimitriou, R. Bhagwan, N. Chandran, R. Ramjee, A. Haeberlen, H. Singh, A. Modi, and S. Badrinarayanan, “Big data analytics over encrypted datasets with seabed,” in Proc. of 12th USENIX OSDI, 2016, pp. 587–602.
2. InfluxDB, “InfluxDB Cloud,” [Online]: Accessed on February 06, 2021, https://www.influxdata.com/.
3. L. Wang, Z. Yang, and X. Song, “SHAMC: A secure and highly available database system in multi-cloud environment,” Future Generation Computer Systems, vol. 105, pp. 873–883, 2020.
4. Y. Hu, S. Kumar, and R. A. Popa, “Ghostor: Toward a secure datasharing system from decentralized trust,” in 17th USENIX NSDI, 2020, pp. 851–877.
5. L. Burkhalter, A. Hithnawi, A. Viand, H. Shafagh, and S. Ratnasamy, “Timecrypt: Encrypted data stream processing at scale with cryptographic access control,” in Proc. of 17th USENIX NSDI, 2020, pp. 835– 850.
6. D. Catalano and D. Fiore, “Practical homomorphic message authenticators for arithmetic circuits,” J. of Cryptology, vol.

Received: 20-09-2025 | Accepted: 24-10-2025 | Published: 31-10-2025 |

31, no. 1, pp. 23–59, 2018.
7. A. Kiayias, S. Papadopoulos, N. Triandopoulos, and T. Zacharias, “Delegatable pseudorandom functions and applications,” in Proc. of 20th ACM CCS, 2013, pp. 669–684.
8. W. Kleiminger, C. Beckel, and S. Santini, “Household occupancy monitoring using electricity meters,” in Proc. of ACM UbiComp, 2015, pp. 975–986

Received: 20-09-2025 | Accepted: 24-10-2025 | Published: 31-10-2025 |