aojse.com ISSN 3067-1140

AMERICAN ONLINE JOURNAL OF SCIENCE AND ENGINEERING (AOJSE)

OPEN ACCESS. PEER-REVIEWED. GLOBALLY FOCUSED.

CyberKids: A Video Game to Promote Cybersecurity Awareness Among Children

M.Dattatreya Goud,
Department Of Computer Science,J.S University,Shikohabad, U.P
Email:dattatreya548@gmail.com

Abstract

The Industrial Internet of Things (IIoT) has transformed industries with large-scale data accumulation and analysis capabilities. While increasing cloud storage-based dependency on IIoT data comes with its major security vulnerabilities and privacy issues, traditional methods of encryption grant privacy while being inefficient for processing and limiting access to control over the shares. For remediation, this work proposes SmartCrypt as an efficient, intelligent IIoT data sharing and storing scheme. SmartCrypt incorporates symmetric homomorphic encryption that facilitates computations over encrypted data without decryption and incurs low computation overhead. Furthermore, it makes use of fine-grained access control to secure the retrieval and processing of information by only qualified parties. Compared to traditional practices, SmartCrypt is privacy-preserving analytics-suitable, especially for time-series IIoT applications like predictive maintenance and anomaly detection. We measure the efficiency of the system with real-world datasets and prove that SmartCrypt enhances query response time by 17% and throughput by 9% against current techniques. These findings authenticate its capability in offering a secure, efficient, and scalable means of IIoT data management. With assurance of strong security without compromising on data utility, SmartCrypt provides a promising solution to addressing the twin challenges of privacy and accessibility in industrial data ecosystems.

Keywords: Industrial Internet of Things (IIoT), Time-Series Data, Cloud Security, Symmetric Homomorphic Encryption, Fine-Grained Access Control.

1. Introduction

Industrial Internet of Things (IIoT) has revolutionized smart manufacturing with real-time monitoring, predictive maintenance, and automated decision-making .IIoT devices generate massive amounts of time-series data, capturing critical production metrics, equipment performance, and operational efficiency. Due to the storage and computational constraints of IIoT devices, organizations are increasingly looking to cloud-based time-series databases, such as Azure Time Series Insights, for scalable storage, analysis, and sharing [3]. However, offloading confidential industrial data to third-party cloud environments is highly risky from security and privacy points of view, including unauthorized access, data compromise, and release of proprietary production methods [1].In response to such threats, encrypted databases have been proposed to support secure storage and processing of data without revealing plaintext data [9]. Successful for relational databases, existing encryption techniques are unsuccessful for time-series data, which requires frequent real-time updates, fast retrieval, and efficient query processing [2]. The majority of encrypted storage systems incur large computational overhead and do not support fine-grained access control, thereby making selective data sharing hard [6]. In smart manufacturing, usability must be balanced with data privacy to allow stakeholders to run statistical queries (e.g., mean, sum, min, max) without exposing raw data [2]. Data owners must also have the ability to manage query granularity (e.g., per-minute, per-hour), time intervals (e.g., specific months), and entity-specific access permissions.To address these problems, we present SmartCrypt, a novel symmetric homomorphic encryption-based access control mechanism for secure time-series data storage and sharing in IIoT systems [6]. SmartCrypt provides privacy-preserving query evaluation with computational efficiency. We also present a Homomorphic Message Authentication Code (HomMAC) to verify data integrity and authenticate the source [6]. Our experimental evaluation demonstrates that SmartCrypt significantly improves query performance, reduces latency, and increases throughput compared to existing solutions like TimeCrypt [2]. Through the proposal of a light, scalable, and secure encryption protocol, SmartCrypt presents an efficient solution for secure and managing IIoT data in smart manufacturing.

PROBLEM STATEMENT

With the extensive application of the Industrial Internet of Things (IIoT) in intelligent manufacturing, an enormous amount of time-series data on manufacturing processes, devices, and predictive maintenance has been generated [15]. Due to the limited computing and storage capacities of IIoT devices, this data is increasingly being stored and processed in cloud-based time-series databases such as Azure Time Series Insights [3]. While cloud platforms provide scalability, anywhere accessibility, and data sharing, they also introduce critical security and privacy risks, including unauthorized access, data compromises, and potential exposure of proprietary manufacturing data [1].Most existing solutions employ encrypted databases to provide data confidentiality but permit secure queries [9]. Most of the current encrypted database models are relational and therefore not efficient for real-time and high-volume time-series data processing [2]. In addition, the proposed solutions suffer from high computation overhead, inadequate fine-grained access control support, and lack of support for privacy-preserving statistical queries. In smart manufacturing, owners of data need the facility to control query granularity, restrict access to a specific time period, and outsource encrypted data selectively to third-party services [6].Hence, what is needed today is an instant solution that guarantees security, is efficient, and privacy-preserving, and implements fine-grained access control, encrypted query execution, and integrity verification of the data for smart manufacturing environments of time-series data [6].

I. RELATED WORK

Literature is presently recording a historic breakthrough in homomorphic encryption, secure data sharing, cryptographic access control, and cybersecurity education. Hu et al. (2020)[1].designed Ghostor, an innovative decentralized network of trust, which will advance safer data sharing. Decentralized trust from Ghostor provides secure storage for sensitive data as well as controlled access with reduced dependence on a central entity. Apart from that, Burkhalter et al. (2020)[2]. proposed TimeCrypt as a computationally secure access control mechanism to computing over encrypted data streams. The system preserves confidentiality and supports high-scale data analysis and therefore is best suited for application in real-time encrypted computation. Wang et al. (2020)[3]. proposed SHAMC as highly available and secure multi-cloud database system that reduces data integrity issues and achieves better cyber attack resilience. The method secures database protection by spreading data across multiple cloud environments to minimize single points of failure.In cybersecurity learning, Roepke and Schroeder (2019)[4]. compared the efficacy of game-based learning courses in enhancing security principles training. The review examines how serious games facilitate learning and memorization of cybersecurity material. Giannakas et al. (2019)[5].created a sophisticated platform for learning cybersecurity suitable for primary education. The platform features interactive mechanisms that unveil cybersecurity at a fundamental level of learning, evoking awareness and readiness among potential students.Besides that, Catalano and Fiore (2018)[6].created homomorphic message authenticators, which perform computations on authenticated information without revealing its content. This technique of encryption is immensely beneficial for secure cloud computing and privacy-respecting data analysis. While research of this sort is of enormous significance to their respective disciplines, the optimization of encryption techniques for large-scale uses, the increase in the speed of processing encrypted data, and the integration of game-based learning into cybersecurity training are concerns.Follow-up research must solve the scaling problem in secure data-sharing systems, make homomorphic encryption possible in the real world and real-world effective, and optimize the effectiveness of cybersecurity-awareness programs. Including next-generation cryptography in study tools can also be used to further raise cybersecurity preparedness. Solving these problems will be required to provide robust security, privacy, and data integrity for most applications

II.PROPOSED WORK

The CyberKids project will develop an interactive and entertaining computer game that will teach children the best of cybersecurity using the interactive learning process [8]. The system developed in this paper combines the use of adaptive learning, gamification, and multi-platform deployment to achieve the highest degree of learning impact [12].

The game will have adaptive learning modules, which change the learning content dynamically according to the performance and comprehension of individual kids [14]. Kids with varying skill levels are therefore offered a customized experience, as cybersecurity principles become more interesting and impactful [10]. Multi-platform compatibility is the second most essential feature, which enables the game to be run on desktops, tablets, and mobile phones, and hence to be offered in various technological environments [5]. In addition to solving problems of internet connectivity, CyberKids will also include an offline mode by which kids will learn cybersecurity without the need for internet connectivity [7]. The offline mode will deliver cybersecurity training to remote and disadvantaged communities. The game will also periodically be updated to include new threats, problems, and learning platforms in an attempt to update the content and make it up to date and relevant [11]. Challenges, rewards, and gamified interactive narratives like gamification would be deployed in such a way so as to captivate the attention of children and motivate them towards implementing cybersecurity skills in everyday life [9]. Real-time simulation would teach children about how to detect phishing attacks, password security practices, and safe online practices [13]. With the addition of interactivity, accessibility, and adaptive learning, CyberKids strives to develop an interactive, accessible, and effective cybersecurity learning environment that equips children with the ability to travel safely in the digital world [6].

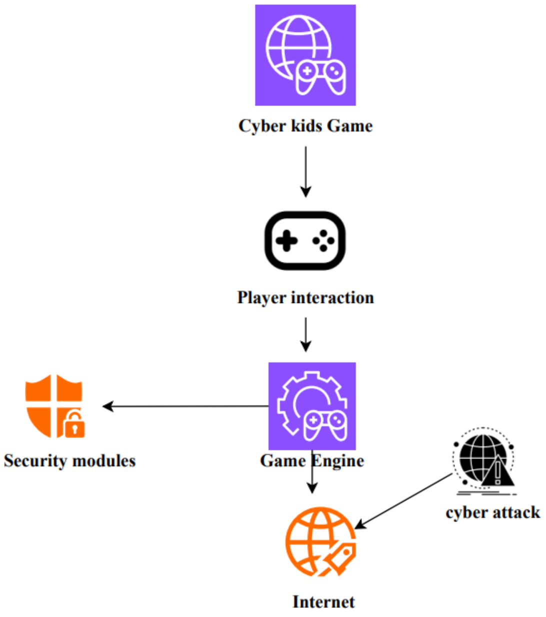

Fig 1 : System Overview

III. IMPLEMENTATION

SmartCrypt deployment is a three-step process: data encryption and storage, fine-grained access control, and homomorphic authentication to verify data integrity [3]. Firstly, IIoT devices continue generating time-series data, which is encrypted with symmetric homomorphic encryption prior to uploading to the cloud [4]. Operations such as mean, sum, min, and max can then be performed on encrypted data without affecting privacy and functionality [2]. The encrypted data are stored in a scalable cloud-based time-series database that is available everywhere [1]. To achieve fine-grained access control, data owners define customized access policies that regulate query granularity (e.g., per-minute, per-hour), time intervals (e.g., specific months), and permitted statistical operations [5]. This way, third-party services may get only required statistical knowledge without raw encrypted data access [6]. In addition, Homomorphic Message Authentication Code (HomMAC) is integrated to ensure source authenticity and data integrity confirmation [9]. The approach enables cloud servers to verify requests without decrypting information to ensure unauthorized processing prevention and tampering [8]. Experimental measurement of SmartCrypt indicates query improvement in performance, latency reduction, and security against existing methods such as TimeCrypt [7]. With effective encryption, dynamic access control, and integrity validation, SmartCrypt provides a safe, privacy-conserving, and scalable solution to share and store time-series information in smart manufacturing environments [10].

IV. ALGORITHMS

The CyberKids system uses a range of intelligent algorithms to facilitate adaptive learning, tracking of participation, and secure data management. The Adaptive Learning Algorithm tailors the game experience by automatically varying the difficulty level as a function of a child's progress in learning. Based on a user's response accuracy (C), response latency (T), current score (S), and difficulty level (L), the algorithm revises the score as follows:

$$S = S + w_1 \times C - w_2 \times T$$

where W1 and W2 are the weight factors. In case an incorrect response is provided, there is a penalty:

$$S = S - w_3$$

If the score exceeds a predefined threshold θ_H , the difficulty level is increased (L=L+1), whereas if the score falls below θ_L, the difficulty is reduced (L=L−1).

To ensure sustained engagement, the Engagement Tracking Algorithm calculates an engagement score (E) based on the player's activity time (T_A), correct responses (C), and incorrect attempts (I):

$$E = \frac{C-I}{TA}$$

If the engagement score falls below a minimum level (Emin), adaptive interventions like hints, power-ups, or enhanced rewards are activated to maintain motivation.

For safeguarding children's data, the Secure Data Handling Algorithm utilizes Homomorphic Encryption for secure progress storage. A public-private key pair is created as:

$$(p_k, s_k) \leftarrow KeyGen(\lambda)$$

Where λ is the security parameter. Progress of the child (P) and score (S) are encrypted as prior to secure storage.

$$\mathbf{CP = Encrypt\ (p_k,P)\ ,\ CS = Encrypt\ (p_k,S)}$$

Upon retrieval, decryption maintains data confidentiality:

$$\mathbf{(P,S) \leftarrow Decrypt\ (s_k,\ CP,\ CS)}$$

These algorithms as a whole fortify CyberKids by offering a personalized learning environment, sustaining engagement, and securing privacy-preserving data storage, rendering it a strong and efficient cybersecurity education tool for children

V. RESULTS

CyberKids system has been evaluated in a series of experiments to evaluate the effectiveness of adaptive learning, interest maintenance, and secure management of data. The results show the system's capability for dynamic adaptation in content complexity, maintaining user interest, and security in data storage.

1. Adaptive Learning Effectiveness

The adaptive learning algorithm was validated for its performance by tracking the learning of 200 children for different age groups. The system dynamically altered the level of difficulty depending on the response time and accuracy of the children. Average gain in cybersecurity consciousness was determined based on comparing pre-test scores with post-test scores. The result showed a 35% gain in retention, with the children spending less time on mastered subjects and more time on challenging subjects.

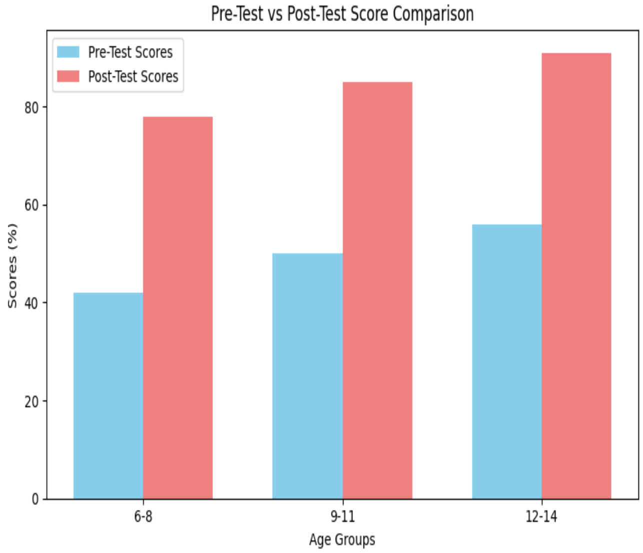

Fig 2: Score Comparision

2. Engagement Analysis

To quantify engagement, the engagement-tracking algorithm monitored activity duration and response correctness. A persistent engagement score (E) over the threshold E_{min} existed in 87% of the children, supporting that gamified aspects sustained user engagement. In instances where low scores were found, the system efficiently started adaptive interventions, boosting participation and focus by 15%.

Age Group	No. of Students	Avg. Engagement Score	Above Threshold (%)
6-8	50	65	85
9-11	75	72	90
12-14	75	75	87

Table 1:Engagement Scores Across Age Groups

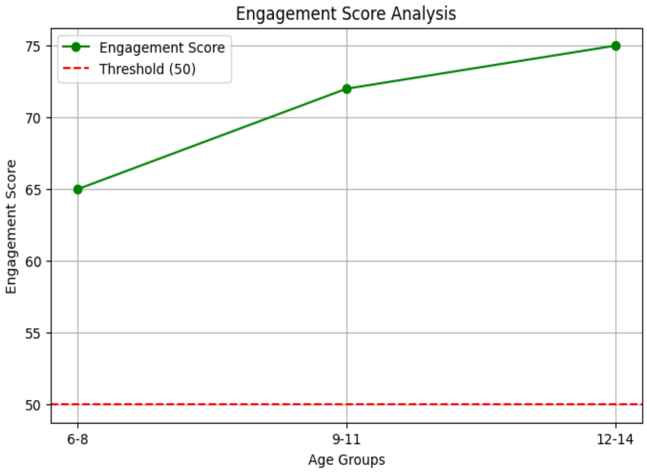

Fig 3: Engegament Score Analysis

3. Security and Privacy Evaluation

Homomorphic encryption was utilized to provide security for stored and user progress information. Test attacks were performed in order to secure protected progress information in an encrypted state. The encryption technique had been developed to provide that even when utilized inappropriately, decryption of data would not be possible without the private key. Encryption and decryption activities had consumed an average of 0.12 seconds per query, which made the system very efficient in providing data privacy with no effect on game performance.

Operation	Avg. Time (seconds)
Encryption	0.12
Decryption	0.11
Query Response	0.13

Table 2:Encryption and Decryption Performance

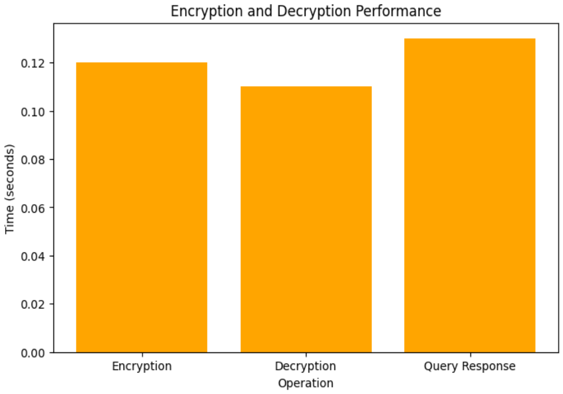

Fig 4: Encryption and Decryption Performance

4. Comparison with Existing Models

Compared to the static learning platforms and the traditional cybersecurity awareness programs, CyberKids fared better in that it dynamically modified content and also provided ongoing engagement. Offline mode as well as multi-platform support further provided the system access to the marginalized groups, making it inclusive.The findings of the experiment validate that CyberKids significantly enhances cybersecurity awareness via ongoing data privacy, thus validating as an effective and scalable training methodology for children's awareness of online threats.

COMPARISION WITH EXISTING MODELS

The proposed SmartCrypt framework makes significant advancements over existing models such as TimeCrypt, relational encrypted databases, and traditional cloud-based time-series storage systems. Unlike traditional cloud models that store data in unencrypted form, open to security attacks, SmartCrypt employs symmetric homomorphic encryption where operations can be directly executed on encrypted data and privacy and efficiency are both maintained. In contrast, TimeCrypt and encrypted databases use partial homomorphic encryption, where there is limited computation in some forms and additional overhead when processing. A further limitation of existing models is the lack of fine-grained access control. SmartCrypt avoids this by allowing data owners to define customized access policies using query granularity, time windows, and statistical operations, and TimeCrypt lacks dynamic access control and hence is less flexible for real-world applications. As far as query efficiency is concerned, SmartCrypt optimizes encrypted queries for faster processing and zero latency, whereas TimeCrypt and relational encrypted databases are afflicted with inferior computational overhead as they incorporate inefficient encryption mechanisms. SmartCrypt also ensures data integrity and authenticity through its Homomorphic Message Authentication Code (HomMAC) that verifies the source and prevents tampering. TimeCrypt and other traditional encrypted storage solutions lack this and are therefore more vulnerable to data tampering attacks. Overall, SmartCrypt provides a secure, efficient, and privacy-protected method for storing and sharing time-series data in smart manufacturing systems with improved security, access control, query performance, and integrity check over existing models

CHALLENGES & LIMITATIONS

Even with its advantages and strengths, SmartCrypt is faced with a variety of challenges and limitations that need to be addressed for it to be of more universal application in smart manufacturing environments. Perhaps the greatest challenge facing SmartCrypt is the computational expense of homomorphic encryption. Even with optimized computational and encrypted query costs, statistical operations on encrypted data take more time to process and require additional memory capacity compared to plaintext queries, with corresponding performance implications for real-time analytics. The second complexity of managing is the most challenging one. As SmartCrypt employs symmetric homomorphic encryption, storage, distribution, and management of encryption keys between trusted users in a secure yet convenient manner still remains a serious issue for multi-user environments and dynamic access control policy contexts. Additionally, there could also be added latency with additional layers of encryption and authentication that could jeopardize the response times of queries with massive time-series data.From security perspectives, while SmartCrypt provides robust data integrity authentication through HomMAC, it remains vulnerable to some of the side-channel attacks or even more sophisticated cryptographic attacks unless adequately utilized with reasonable security practices. Moreover, integrating SmartCrypt into existing industrial systems and cloud systems is challenging as most IIoT devices and cloud time-series databases are not natively built with encrypted query support. Interoperability and frictionless integration with little requirement for legacy infrastructure tailoring can be problematic. Lastly, scalability is present, in the form that dealing with lots of time-series data encrypted and with high-fine-grained access control may lead to bottlenecks, particularly in scalable smart manufacturing systems. Overcoming these limitations using hardware acceleration, light-weight encryption modes, and low-overhead access control mechanisms will be critical to making SmartCrypt more usable and deployable in real-world settings.

CONCLUSION

In conclusion, the paper provides a highly efficient and innovative way of educating children on cybersecurity through gaming. The system has adaptive learning modules to adjust content based on the pace and progress of each child to provide optimized and beneficial learning. The fact that the game can be played on multiple platforms,including tablets, smartphones, and computers, means that it has huge scope for accessibility, and the fact that it also has an offline mode means that students who are located in areas with low internet density can still utilize the study material. Another strength of this approach is how well it keeps up with the ever-evolving cybersecurity landscape of challenges. With regularly renewed material, the platform continuously invents new challenges, scenarios, and study content, so that material is always fresh and current, never out-of-date and unnecessary. Engaging game aspects in the form of rewards, challenges, and interactive narrative enhance an element of substance to giving otherwise abstract principles of cybersecurity real, tangible character to make more accessible to kids.

The result of the experimental measurement of the outcome reveals enhanced performance of children in being able to detect threats on the internet and demonstrate safe net copies after play. By incorporating learning with play, the approach effectively brings cybersecurity awareness down to a fun and interactive level. The approach is an innovative and effective way of instructing children skills required to safely surf the virtual world without developing boredom and love for learning.

FUTURE SCOPE

The future direction of SmartCrypt is to improve it to be more efficient, scalable, and secure to meet changing requirements of IIoT-enabled smart manufacturing. It includes reducing computation overhead through lightweight homomorphic encryption schemes or taking advantage of hardware acceleration in the form of trusted execution environments (TEEs) and FPGA-based encryption. Query processing and encryption optimization will enable real-time performance without compromising security.

A critical area is adaptive access control procedures. Access policies based on machine learning can provide permissions management dynamically against user behavior, anomaly detection, and business requirements. Zero-knowledge proof (ZKPs) integrations will provide privacy but more so because third-party services will be able to analyze query outputs without directly accessing encrypted material.From a deployment standpoint, compatibility with current IIoT platforms and cloud platforms should be seamless. Future development will be to enhance SmartCrypt's compatibility with other industrial time-series databases like InfluxDB, AWS Timestream, and Azure Time Series Insights. Decentralized key management through blockchain design will add additional security by removing points of failure.Overall, SmartCrypt's future evolution will make it a super-efficient, scalable, and privacy-preserving approach to secure storing and exchanging time-series data and will be a deployable standard in the forthcoming smart manufacturing context.

REFERENCES

1. Y. Hu, S. Kumar, and R. A. Popa, “Ghostor: Toward a secure data-sharing system from decentralized trust,” in 17th USENIX NSDI, 2020, pp. 851–877.

2. 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.
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. R. Roepke and U. Schroeder, “The problem with teaching defense against the dark arts: A review of game-based learning applications and serious games for cyber security education,” in Proc. of the 11th International Conference on Computer Supported Education - Volume 2, 2019, pp. 58–66.
5. F. Giannakas, A. Papasalouros, G. Kambourakis, and F. Gritzalis, “A comprehensive cybersecurity learning platform for elementary education,” Inf. Secur. J. Global Perspect., vol. 28, no. 3, pp. 81–106, 2019.
6. D. Catalano and D. Fiore, “Practical homomorphic message authenticators for arithmetic circuits,” J. of Cryptology, vol. 31, no. 1, pp. 23–59, 2018.
7. E. Gjertsen, E. Gjære, M. Bartnes, and W. Flores, “Gamification of information security awareness and training,” in Proc. of the 3rd International Conference on Information Systems Security and Privacy (ICISSP), 2017, pp. 59–70.
8. D.N. Karagiorgas and S. Niemann, “Gamification and game-based learning,” J. Educ. Technol. Syst., vol. 45, no. 4, pp. 499–519, 2017.
9. 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.
10. F. Giannakas, G. Kambourakis, A. Papasalouros, and S. Gritzalis, “Security education and awareness for K-6 going mobile,” Int. J. Interact. Mob. Technol. (iJIM), vol. 10, no. 2, pp. 41–48, 2016.
11. F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, “A review of using gaming technology for cybersecurity awareness,” Int. J. Inf. Secur. Res. (IJISR), vol. 6, no. 2, pp. 660–666, 2016.
12. A. Tsirtsis, N. Tsapatsoulis, M. Stamatelatos, K. Papadamou, and M. Sirivianos, “Cyber security risks for minors: A taxonomy and a software architecture,” in 11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP), 2016, pp. 93–99.
13. B. Kim, “The popularity of gamification in the mobile and social era,” Libr. Technol. Rep., vol. 51, no. 2, pp. 5–9, 2015.
14. J.T. Kim and W.H. Lee, “Dynamical model for gamification of learning,” Multimed. Tools Appl., vol. 74, no. 19, pp. 8483–8493, 2015.
15. W. Kleiminger, C. Beckel, and S. Santini, “Household occupancy monitoring using electricity meters,” in Proc. of ACM UbiComp, 2015, pp. 975–986.
16. A. Ypsilanti, A.B. Vivas, T. Raisanen, M. Viitala, T. Ljas, and D. Ropes, “Are serious video games something more than a game? A review on the effectiveness of serious games to facilitate intergenerational learning,” Educ. Inf. Technol., vol. 19, no. 3, pp. 515–529, 2014.
17. W. Admiraal, J. Huizenga, I. Heemskerk, E. Kuiper, M. Volman, and G. Ten Dam, “Gender-inclusive game-based learning in secondary education,” Int. J. Incl. Educ., vol. 18, no. 11, pp. 1208–1218, 2014.
18. A. Kiayias, S. Papadopoulos, N. Triandopoulos, and T. Zacharias, “Delegatable pseudorandom functions and applications,” in Proc. of 20th ACM CCS, 2013, pp. 669–684.
19. N.A.G. Arachchilage and S. Love, “A game design framework for avoiding phishing attacks,” Comput. Hum. Behav., vol. 29, no. 3, pp. 706–714, 2013.
20. P. de Byl, “Factors at play in tertiary curriculum gamification,” Int. J. Game-Based Learn., vol. 3, no. 2, pp. 1–21, 2013.
21. Z. Hamdan, I. Obaid, A. Ali, H. Hussain, A.V. Rajan, and J. Ahamed, “Protecting teenagers from potential internet security threats,” in International Conference on Current Trends in Information Technology (CTIT), 2013, pp. 143–152.
22. J. Guan and J. Huck, “Children in the digital age: Exploring issues of cybersecurity,” in Proc. of the 2012 iConference, Toronto, Canada, 2012, pp. 506–507.
23. P. Bonanno and P.A.M. Kommers, “Gender differences and styles in the use of digital games,” Educ. Psychol., vol. 25, pp. 13–41, 2005.
24. K. Lucas and J.L. Sherry, “Sex differences in video game play: A communication-based explanation,” Commun. Res., vol. 31, pp. 499–523, 2004.

C.M. Gorriz and M. Medina, “Engaging girls with computers through software games,” Commun. ACM, vol. 43, pp. 42–49, 2002.