ISSN: 2182-2069 / E-ISSN: 2182-2077

Privacy-Aware Information Security for E-Learning Platforms in History Using Attribute-Based Encryption Algorithm

Muslihiddin Muhiddinov[1*], Nizomiddin Ochilov[2], Bekpulat Umurkulov[3], Umid Kholnazarov[4], Ibrokhim Sapaev[5], Nigina Bazarova[6], Muyassar Kholova[7], and Gulnora Aripova[8]

[1*]Doctor of Philology, Professor of the Department of Classical Literature History, Samarkand State University, Uzbekistan. muhiddinovmuslihiddin1@gmail.com, https://orcid.org/0009-0002-2071-8645

[2]Kimyo International University in Tashkent, Tashkent, Uzbekistan. n.ochilov@kiut.uz, https://orcid.org/0000-0002-7486-9441

[3]Doctor of Philology, Professor of Department of Uzbek Linguistics, Termez State University, Uzbekistan. umurqulovb@tersu.uz, https://orcid.org/0000-0003-2348-2682

[4]PhD, Senior Lecturer of Department of Uzbek Linguistics. Termez State University, Termez, Uzbekistan. xolnazarovu@tersu.uz, https://orcid.org/0009-0003-6126-1140

[5]Head of the Department Physics and Chemistry, "Tashkent Institute of Irrigation and Agricultural Mechanization Engineers" National Research University, Tashkent, Uzbekistan; Scientific Researcher, University of Tashkent for Applied Sciences, Str. Gavhar 1, Tashkent, Uzbekistan; Western Caspian University, Scientific Researcher, Baku, Azerbaijan. sapaevibrokhim@gmail.com, https://orcid.org/0000-0003-2365-1554

[6]Associate Professor of the Department of Pharmaceutical Business Organization, Samarkand State Medical University, Uzbekistan. bozorovanigina72@gmail.com, https://orcid.org/0009-0006-1391-0283

[7]Professor of Department of Uzbek Linguistics, Termez State University, Termez, Uzbekistan. xolovam@tersu.uz, https://orcid.org/0000-0002-7604-2958

[8]Professor, Tashkent Institute of Chemical Technology, Uzbekistan. shuhgul711@gmail.com, https://orcid.org/0000-0001-5731-6071

Received: December 04, 2024; Revised: January 14, 2025; Accepted: January 27, 2025; Published: February 28, 2025

Abstract

The swift progression of technological advances has made Digital Instructional Resources (DIR) more critical in the history of E-Learning. Conventional access control methods inadequately address the need for fine-grained distribution of DIR in intricate educational settings. The research employs Attribute-Based Encryption (ABE) grounded in ciphertext rules. It integrates it with Blockchain (BC)'s decentralized and tamper-proof characteristics to formulate a secure sharing design that merges BC with ABE Privacy-Aware Information Security (P-IS) methods. This facilitates the safe and meticulously regulated sharing of history E-Learning materials. The results

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 1 (February), pp. 305-315.
DOI: *10.58346/JISIS.2025.I1.019*

*Corresponding author: Doctor of Philology, Professor of the Department of Classical Literature History, Samarkand State University, Uzbekistan.

indicate that the developed model's mean encryption and decryption times were 1.77 seconds and 1.76 seconds, respectively. Compared to ABE key regulations encoding and policy-based ABE, the mean encryption period decreased by 0.76 seconds and 2.72 seconds, while the standard decryption time decreased by 0.80 seconds and 2.15 seconds, demonstrating superior efficiency in processing duties. The ciphertext upload duration of the developed model stays invariant at 9.3 ms, demonstrating its superior scalability for additional users without augmenting delay. The design model keeps the ciphertext length short even as the number of traits increases. This shows that it can significantly reduce the storage space needed and improve the whole system. The method solves the problems with sharing data in E-Learning and can be used as a model in other areas that need to protect information.

Keywords: E-Learning, Attribute-Based Encryption, Privacy, Information Security.

1 Introduction

As schooling worldwide becomes more computerized, E-Learning materials have become essential to the new school system (Singh et al., 2021). Because these things are so common, varied, and easy to get, they have changed how schools usually work. Privacy-Aware Information Security (P-IS) (Al-Hawawreh & Hossain, 2023) lets students and teachers work together without being limited by time or space to get quick access to information and work together interactively (Ranieri et al., 2021). Learners have successfully incorporated cell phones and programs into their daily lives, using apps on their phones for various social, private, and educational purposes (Majid et al., 2024). As the amount of data being sent and received quickly grows, schools' problems with managing resources and Secure Sharing (SS) have become more critical (Aravind et al., 2023). Protecting personal information and intellectual property rights (IPR) while making the best use of resources has become a big problem for innovative learning.

To protect the needs of content creators and students, educational organizations must make sure that private data is kept safe from people who shouldn't have access to it and that Digital Instructional Resources (DIR) aren't copied or shared without permission (Thongmeensuk, 2024). The academic DIR resource-sharing method needs to be personalized and changed to keep up with the history of variety and individualization in E-Learning (Gal-Oz et al., 2010). Changing the traditional centralized management model to fit these needs is hard, and putting BC into place is a new way to solve the P-IS problem (Salman & Alomari, 2023). BC's main perks are decentralized, open, and safe. It can provide tamper-proof records for ER storage and use distributed ledger technology to show where information came from (Saranya & Madhubala, 2019). The Attribute-based Encryption (ABE) method gives the system a more complex and flexible way to manage who can access your resources (Jeneba Mary et al., 2024). Both the ABE method and the BC method for P-IS are used in this work (Qader & Turkben, 2022). Through Specific-Policy ABE (SP-ABE) (He et al., 2021), ciphertext management is added to the ABE architecture to create an SS system for digital records (Li et al., 2023).

This idea combines BC's unchangeable and decentralized features with the SP-ABE method's granular encryption approach in a new and creative way (Sethuraman & Radhakrishnan, 2024). This opens up new possibilities for innovative school data management and ensures that history E-Learning resources can be shared safely (Udayakumar et al., 2023). This method can help academic schools grow in a way that doesn't harm the environment, and it can also be used as a model for similar problems that come up in other areas (Sharma & Nair, 2025). There are five parts to the study. The first part outlines the history of the E-Learning Resources (ER), BC, and ABE algorithms.

2 Background

Because of the growth of e-learning, DIRs are now an essential part of modern teaching. There are significant risks to the academic ecosystem from unauthorized entry, data breaches, and IPR violations. Scholars have put forward many ideas for how to solve these problems. Using Deep Reinforcement Learning (DRL) (Li et al., 2023), the study found a quick way to find IPR violations. This technique uses deep Q-learning and Artificial Neural Network (ANN) methods (Kurani et al., 2023) to find safe watermarked locations close to the original idea. This speeds up the training of vectors of features. The study team created a BC-based organization for storing and sharing information to protect privacy and get student educational records to as many people as possible for P-IS. By combining BC with storage systems, this plan ensures that data is stored safely, and the tests show that it lasts a very long time. To solve security problems, the study team created a BC-based e-learning information environment. The results show that this method dramatically shortens the time it takes to find something. A BC-based e-learning tool uses BC to protect learners' privacy, keep e-learning data safe, and stop it from being changed. This shows that the structure makes the e-learning setting fair and transparent for P-IS. The study created a peer-to-peer decentralized Internet of Things (IoT) network (Chen et al., 2022) that works well and is safe. It uses BC to make it easier for connected devices to share information safely.

This design does not need trusted middlemen because untrusted devices can use BC to communicate with other devices in a way that requires no verification. However, the results show that the hash produced by this model is very different from those produced by other encryption methods. To make the ER more open, safe, and private, create a semantic web-based history e-learning content retrieval structure that uses semantic terminology and user queries to make a resource description structure. This will show that the system is new and valuable for P-IS.

A data security exchange method using SP-ABE and BC was created as part of the study to make data trade systems safer. The technique protects the privacy of access policy data by creating the right ciphertext and key architectures and setting up a successful and flexible multi-authorization center control system that makes policy hiding easier. Based on the findings, the approach works very well. The study created a BC-based structure that uses BC to make sure that resource generators are real and stop activities or changes that aren't allowed. The results show that the system can handle ER for P-IS well. They created a BC-based structure that uses BC to ensure that resource providers are accurate and that no one else can change or add to the structure without permission. The results show that the system can effectively handle ER.

The study made a BC-based E-Learning platform to ensure that views are reliable and accurate. The immutability and openness of BC protect resource intellectual property rights while ensuring the system works well. Visibility protects the rights to resources and provides a framework for knowledge exchange and financial transformation. The outcomes show that the platform can successfully keep DIRs safe. The study suggests using a signature-based Rivest Shamir Architecture (RSA) (Panthi & Bhuyan, 2023) to improve information sharing between students and teachers in the school system. It also looks at possible threats damaging data sent through the suggested structure. The results indicate its superior capability in safeguarding data security and enhancing productivity. The study developed a semantic web-based digital educational asset-sharing system based on the internet to address the existing web resource-sharing paradigm. This model utilizes Extensible Markup Language. (XML) (Matulewski et al., 2022) as its foundational syntax and generates pertinent applications using XML tailored to the specificities of teaching resource utilization for P-IS. The results indicate that the framework is practical. The utilization rate of the emergency room is elevated. Numerous scholars have significantly improved the security of

online educational materials and increased the efficiency and stability of resource sharing in e-learning. These methods encounter challenges, including substantial detail and elevated implementation costs.

The study integrates BC with the ABE method. It presents ciphertext rules grounded in the ABE method to develop a BC data access management system utilizing the SP-ABE method to improve system efficiency and customer experience and minimize installation and upkeep costs.

3 Proposed P-IS for E-Learning Platform

The extensive use of P-IS in the history of E-Learning produces substantial DIRs. The conventional centralized design struggles to satisfy the requirements for secure collaboration of resources. The research develops an SS system for DIR by integrating BC with the ABE algorithm to resolve security concerns in sharing for P-IS.

Development of an SS Framework for ER

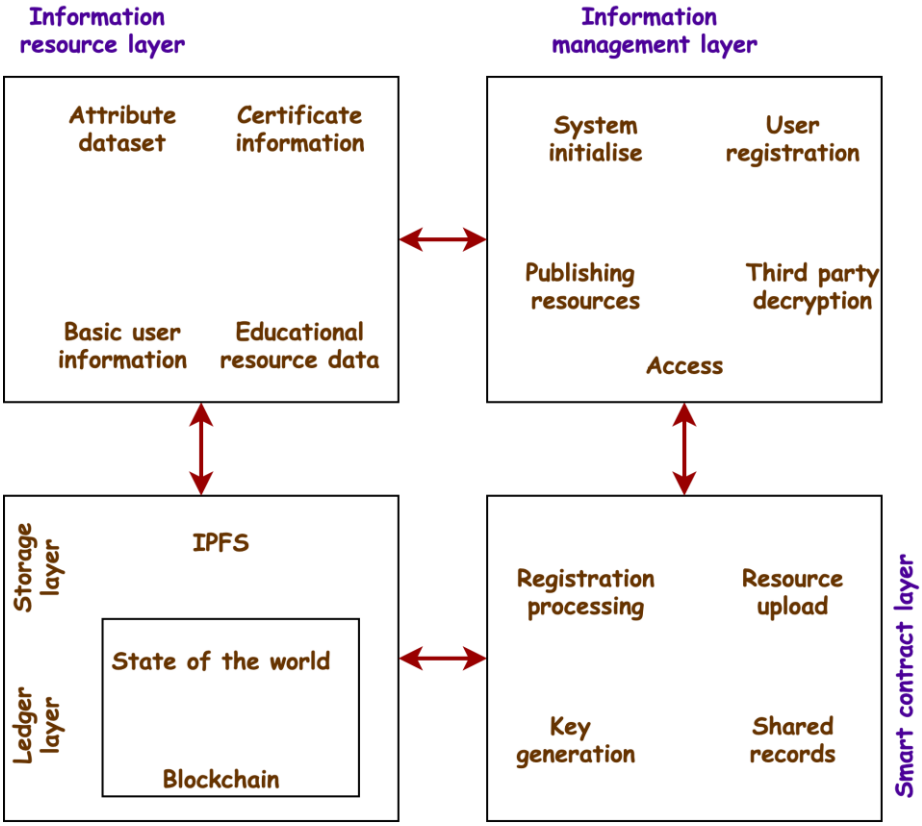

Figure 1: Model System Framework

In the modern information era, the proliferation of DIR has rendered privacy and data protection critical concerns in the design of computer networks. In higher learning, the diverse and specific needs of instructors, pupils, scholars, and other stakeholders require a DIR administration system to possess highly flexible and precise restrictions on access capabilities for P-IS. to facilitate the effective sharing of learning assets while ensuring privacy protection, this research integrates BC with the ABE system to develop a digital curriculum collaboration model, illustrated in Figure 1.

The model incorporates BC with ABE methods to establish a multi-tiered construction comprising an information resource level, an information processing level, an innovative contract level, and a storage level. The information resource level manages and categorizes educational information in many formats, including text, video, test financial institutions and other resources. The data processing layer manages resource distribution reasoning and is accountable for processing user inquiries and application reasoning. It serves as a user-system communication mediator, translating what users want to facilitate the system's functioning. The intelligent contract level employs BC to autonomously implement intricate company regulations, like resource ownership and the allocation of usage freedoms, via intelligent agreements to guarantee transparency and immutability of business logic in history E-Learning. The storage level is accountable for preserving data and ensuring its confidentiality and dependability for P-IS. It encompasses a relational database management tool with encryption to safeguard saved information from unauthorized access. The model's unique structure is illustrated in Figure 2.

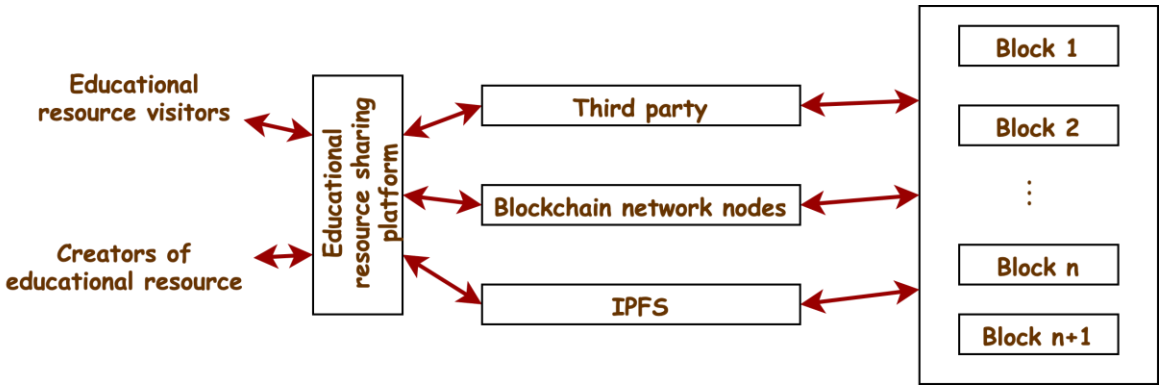

Figure 2: Specific Structural Model

Before utilizing the site, a user must finalize their registration. In this procedure, the user must provide a collection of attributes to the Authorization Center (AC), including identity information, organizational affiliation, and role duties. The AC is tasked with validating the reliability and legitimacy of these attributes. Upon verification, the AC generates relevant attribute keys according to the individual's characteristics. It securely delivers those credentials to the consumer, which will be employed to ascertain the customer's access privileges while accessing protected services. The developer of anDIR must complete a registration procedure akin to a standard user's to acquire an individual feature key before posting the material to the internet for P-IS. The research will thereafter establish an access policy for the asset. This policy delineates the criteria for user attributes permitted to access the asset.

The owner will employ the ABE method to secure the asset according to the specified access policy in history E-Learning. Upon finalizing the encryption, the developer disseminates the protected resource on the platform, accompanied by the corresponding access policy. Applicants must demonstrate that their characteristics conform to the service's use policy while accessing that resource. Visitors are required to submit their attribute key to decode the material. The smart contract will ascertain if the requestor's characteristic key aligns with the resource's accessibility restriction for P-IS. Upon successful examination, the intelligent contract will permit the decryption procedure, enabling the user to access the plaintext asset. The object can be decoded effectively only if the user's characteristic key aligns with the resource's accessibility rule. Figure 3 illustrates the precise flow of the associated process.

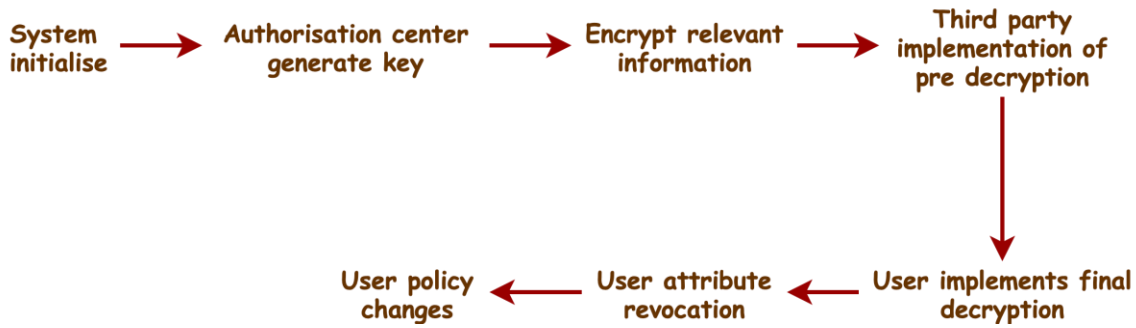

Figure 3: Process of ABE Method

4 Results

This study performs simulations utilizing the JPBC open-source Java library to evaluate the efficacy of the suggested SS model, executed on an Intel processor equipped with 8 GB of RAM and operated on a 32-bit Windows 10 system. Initially, encrypted and decrypted processes are executed on a collection of 140 KB plain texts, with the respective times for these operations measured about those of Key-Policy ABE (KP-ABE) and Specific-Policy ABE (SP-ABE1). The encrypted and decoding durations of Based Encryption and CP-ABE are contrasted with the outcomes illustrated in Figure 4.

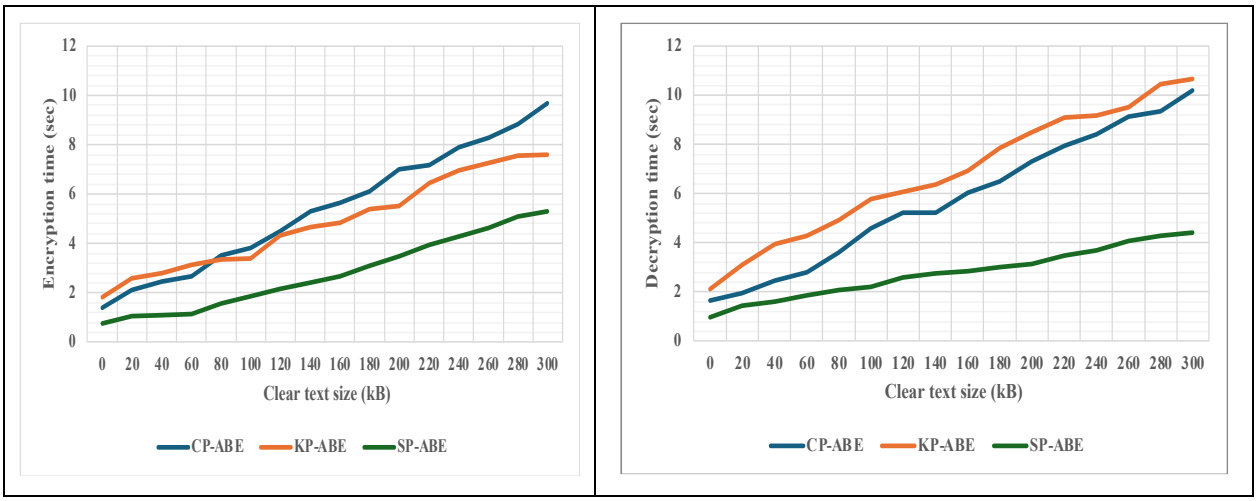

Figure 4: Encryption and Decryption Time Analysis

Figure 6(a) illustrates that the encryption duration of various techniques generally escalates with the augmentation of plaintext size. The CP-ABE method has a median encryption duration of 4.38 seconds, the KP-ABE method has a mean encryption duration of 2.42 seconds, and the SP-ABE method has a mean encryption time of 1.77 seconds. Figure 6(b) illustrates that the decryption time for various techniques escalates with the augmentation of plaintext dimensions, with median decryption times of 3.80 s, 2.45 s, and 1.76 s for the three methods. Compared to the KP-ABE and CP-ABE methods, SP-ABE demonstrates reduced time expenditure in the encoding and decoding procedures, establishing its computational effectiveness superiority for P-IS. To validate the security of the proposed SS approach, the study conducts a comparative analysis with various methods from diverse viewpoints, yielding 1 for supported and 0 for unsupported features in history E-Learning.

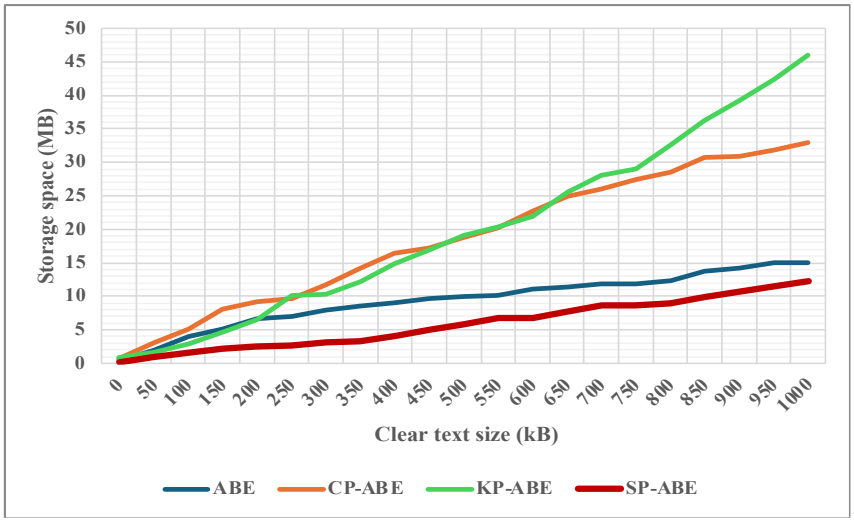

Figure 5: Storage Space Analysis

The proposed SS paradigm fulfills these criteria in four dimensions: fine-grained control of access, safeguarding privacy, effective administration of decoding and encrypting keys, and SS of keys. This indicates its capacity to deliver extensive security while guaranteeing history E-Learning user-friendliness. It demonstrates the capability to offer a thorough, safe, and easy-to-use data-sharing ecosystem. The variance in storage space needed to implement the access control approach, based on the number of individuals using different methods, is computed, and the outcomes are illustrated in Figure 5.

Figure 5 illustrates that when the number of clients increases, the storage space necessary for the access control model across various methods exhibits a consistent rising trajectory. When the user count hits 850, the storage space required for the access control system utilizing the SP-ABE method is 5.0 MB, markedly less than what was needed by alternative methods. The SP-ABE technique alleviates storage demands as the client base expands, maintaining security and enhancing system adaptability in history E-Learning. To validate the safety of the suggested BC access control model utilizing the SP-ABE method, the effectiveness rate of the model versus Sybil attacks, Denial of Service (DoS) attacks, and User Revocation attacks were assessed in a distributed framework compared to KP-ABE and the current system for P-IS.

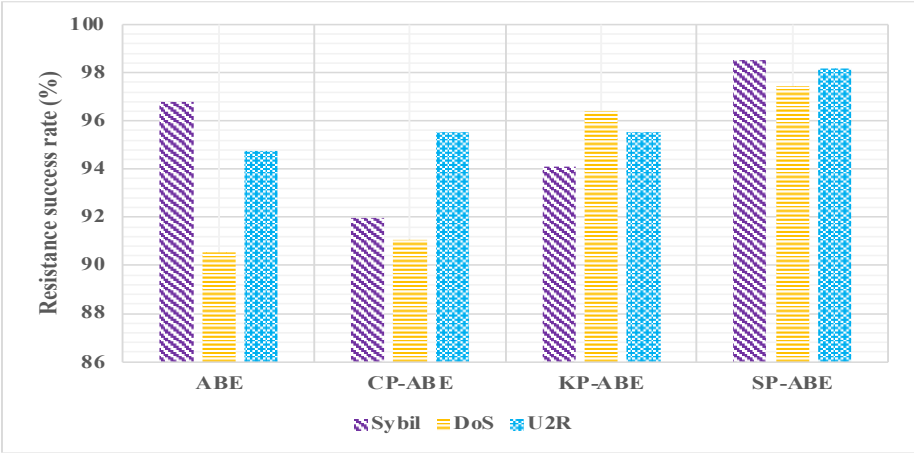

Figure 6: Resistance Success Rate Analysis

Figure 6: indicates that a BC-based authentication model utilizing the SP-ABE method, as described by the research institute, achieves a success rate of 98.15% against Sybil assaults, 96.52% against DoS assaults, and 97.48% against User-to-Root (U2R) assaults. Observations indicate that the suggested approach has a much superior success rate in withstanding three types of attacks compared to the other two alternatives, illustrating its efficacy in countering various network assaults in dispersed contexts for P-IS. A sensitivity study was performed to evaluate the model's reliability and resilience under varying network user burdens, with data leakage rates determined for user inputs of 1000, 2000, and 3000 in the history of E-Learning. The outcomes are depicted in Figure 7.

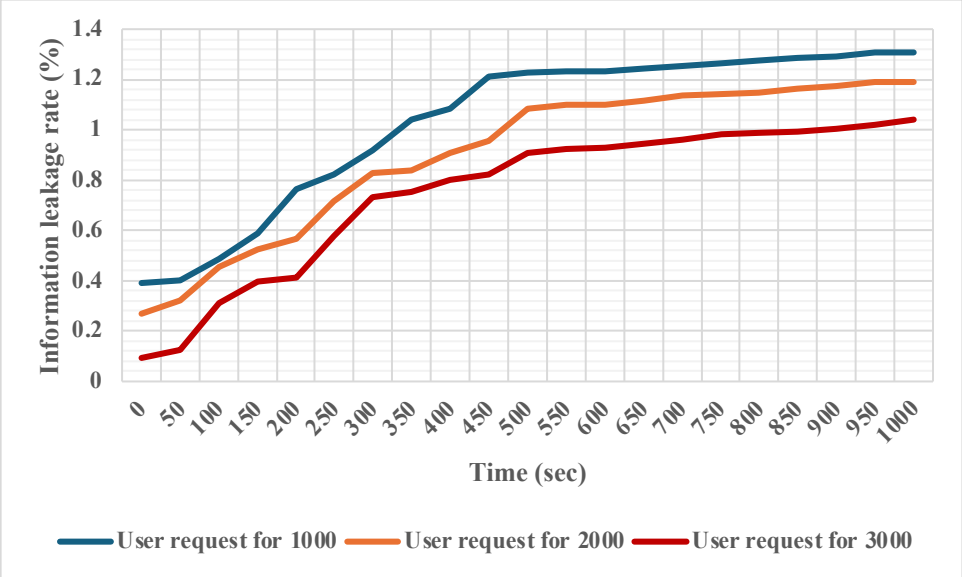

Figure 7: Information Leakage Rate Analysis

Figure 7 illustrates that the Data Leakage Rate (DLR) exhibits an increasing tendency as time progresses and subsequently maintains. When the user demand is 1000, the permitted DLR is 1.32%. When the client's demand is 2000, the highest DLR is 1.53%. When the consumer's demand is 3000, the highest possible DLR is 1.56% in the history of E-Learning for P-IS. As customer inquiries rise, the DLR progressively escalates, albeit decelerating, illustrating the suggested model's resilience and stability under substantial user demands.

5 Conclusion

The safe transmission of digital ER now encounters numerous hurdles, including resource misallocation and piracy issues, significantly impeding ER's proper utilization and dissemination. The research develops an SS system utilizing the ABE method optimized by ciphertext policy and integrated with the BC system to enhance data management refinements while safeguarding data safety and user confidentiality in history E-Learning for P-IS. The results indicate that the SP-ABE method exhibits reduced time consumption for decoding and encrypting, achieving times of 1.77 seconds and 1.76 seconds, greatly enhancing the processing speed compared to the CP-ABE and KP-ABE algorithms. With the user count rising to 850, the necessary storage capacity remains 5.0 MB, demonstrating that the implemented SS architecture mitigates the storage demands associated with scalability for P-IS. The SP-ABE technique maintains a consistent ciphertext size of 5.9 KB and a stable download time of 9.3 ms, even when the number of attributes rises, so it is confirmed to be efficacious in data access

management. The design concept significantly diminishes latency to 0.44 seconds and enhances system capacity to 605.3 bits, demonstrating its efficiency in data processing. The model's efficacy in managing extensive user bases has not been thoroughly proven, and its possibility for storage optimization remains unexamined. The following study will investigate the optimization of methods to accommodate the swift expansion of the user base and broaden the applicability of models for distinct requirements in various historical E-Learning contexts. Particular access control mechanisms are implemented, and BC-based technologies can be refined to facilitate the model's querying of data access data for P-IS. By implementing more stringent control over access and information protection protocols, the concept can be adapted to more domains necessitating safe and precise data sharing to amplify its practical impact.

References

[1] Al-Hawawreh, M., & Hossain, M. S. (2023). A privacy-aware framework for detecting cyber attacks on internet of medical things systems using data fusion and quantum deep learning. *Information Fusion*, *99*, 101889. https://doi.org/10.1016/j.inffus.2023.101889

[2] Aravind, B., Harikrishnan, S., Santhosh, G., Vijay, J. E., & Saran Suaji, T. (2023). An Efficient Privacy - Aware Authentication Framework for Mobile Cloud Computing. *International Academic Journal of Innovative Research*, *10*(1), 1–7. https://doi.org/10.9756/IAJIR/V10I1/IAJIR1001

[3] Chen, Z., Liao, W., Tian, P., Wang, Q., & Yu, W. (2022). A fairness-aware peer-to-peer decentralized learning framework with heterogeneous devices. *Future Internet*, *14*(5), 138. https://doi.org/10.3390/fi14050138

[4] Gal-Oz, N., Grinshpoun, T., & Gudes, E. (2010). Privacy issues with sharing and computing reputation across communities. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *1*(4), 16-34.

[5] He, Y., Wang, H., Li, Y., Huang, K., Leung, V. C., Yu, F. R., & Ming, Z. (2021). An efficient ciphertext-policy attribute-based encryption scheme supporting collaborative decryption with blockchain. *IEEE Internet of Things Journal*, *9*(4), 2722-2733. https://doi.org/10.1109/JIOT.2021.3099171

[6] Jeneba Mary, A., Kuppusamy, K., & SenthilRajan, A. (2024, May). A Comprehensive Analysis of ABE Access Control Mechanisms in Cloud Environment. In *International Conference on Intelligent Communication, Control and Devices* (pp. 337-348). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-97-8329-8_26

[7] Kurani, A., Doshi, P., Vakharia, A., & Shah, M. (2023). A comprehensive comparative study of artificial neural network (ANN) and support vector machines (SVM) on stock forecasting. *Annals of Data Science*, *10*(1), 183-208. https://doi.org/10.1007/s40745-021-00344-x

[8] Li, C., Zheng, P., Yin, Y., Wang, B., & Wang, L. (2023). Deep reinforcement learning in smart manufacturing: A review and prospects. *CIRP Journal of Manufacturing Science and Technology*, *40*, 75-101. https://doi.org/10.1016/j.cirpj.2022.11.003

[9] Majid, U. M. A, Atan, N. A., Rukli, R., & Khan, A. (2024). Framework of Computer Science Learning Through Hybrid Service Learning Oriented Visual Toward the Continuum of Visualization Thinking and Generic Skills. *Indian Journal of Information Sources and Services*, *14*(3), 192–206. https://doi.org/10.51983/ijiss-2024.14.3.25

[10] Matulewski, J., Bałaj, B., Mościchowska, I., Ignaczewska, A., Linowiecki, R., Dreszer, J., & Duch, W. (2022). Learnability evaluation of the markup language for designing applications controlled by gaze. *International Journal of Human-Computer Studies*, *165*, 102863. https://doi.org/10.1016/j.ijhcs.2022.102863

[11] Panthi, S., & Bhuyan, B. (2023, October). Quantum-Resistant Hash-Based Digital Signature Schemes: A Review. In *International Conference on Frontiers in Computing and Systems* (pp. 637-655). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-97-2611-0_43
[12] Qader, A. M., & Turkben, A. K. (2022). Multi Channels Deep Convolution Neural Network for Early Classification of Multivariate Time Series. *International Journal of Advances in Engineering and Emerging Technology, 13*(2), 230–240.
[13] Ranieri, A., Caputo, D., Verderame, L., Merlo, A., & Caviglione, L. (2021). Deep adversarial learning on google home devices. *Journal of Internet Services and Information Security, 11*(4), 33-43.
[14] Salman, R. H., & Alomari, E. S. (2023). Survey: Homomorphic Encryption-based Deep Learning that Preserves Privacy. *International Academic Journal of Science and Engineering, 10*(2), 153–163. https://doi.org/10.9756/IAJSE/V10I2/IAJSE1019
[15] Saranya, U., & Madhubala, P. (2019). Enhancement of security and network lifetime using flexi-cast method. *International Journal of Communication and Computer Technologies, 7*(1), 23-26.
[16] Sethuraman, P., & Radhakrishnan, S. (2024). Examining burnout and stress among healthcare professionals during and post COVID-19 lockdown: A comparative analysis. *Salud, Ciencia y Tecnología-Serie de Conferencias,* (3), 900.
[17] Sharma, A., & Nair, V. (2025). Developing a Medical Coding Curriculum for Surgery Students by Resolving Inconsistencies among Physician and Student Records. *Global Journal of Medical Terminology Research and Informatics, 2*(1), 30-36.
[18] Singh, M., Adebayo, S. O., Saini, M., & Singh, J. (2021). Indian government E-learning initiatives in response to COVID-19 crisis: A case study on online learning in Indian higher education system. *Education and Information Technologies, 26*(6), 7569-7607. https://doi.org/10.1007/s10639-021-10585-1
[19] Thongmeensuk, S. (2024). Rethinking copyright exceptions in the era of generative AI: Balancing innovation and intellectual property protection. *The Journal of World Intellectual Property*, *27*(2), 278-295. https://doi.org/10.1111/jwip.12301
[20] Udayakumar, R., Suvarna, Y.P., Yogesh, M.G., Vimal, V.R., & Sugumar, R. (2023). User Activity Analysis Via Network Traffic Using DNN and Optimized Federated Learning based Privacy Preserving Method in Mobile Wireless Networks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 14*(2), 66-81.

Authors Biography

Muslihiddin Muhiddinov is a distinguished Doctor of Philology and Professor at the Department of Classical Literature History at Samarkand State University. He has made notable contributions to the study and teaching of classical literature.

Nizomiddin Ochilov is an academic at Kimyo International University in Tashkent. His research interests span various disciplines, and he actively contributes to conferences and publications.

Bekpulat Umurkulov is a highly respected Doctor of Philology and Professor at the Department of Uzbek Linguistics at Termez State University. His expertise lies in linguistics, and he has published extensively in the field.

Umid Kholnazarov is a PhD holder and senior lecturer at the Department of Uzbek Linguistics, Termez State University. His work primarily focuses on language studies and pedagogy.

Ibrokhim Sapaev is a prolific multidisciplinary researcher and the Head of the Department of "Physics and Chemistry" at Tashkent Institute of Irrigation and Agricultural Mechanization Engineers. He also collaborates with the University of Tashkent for Applied Sciences and Western Caspian University.

Nigina Bazarova is an Associate Professor at the Department of Pharmaceutical Business Organization, Samarkand State Medical University. She specializes in pharmaceutical business studies.

Muyassar Kholova is a Professor in the Department of Uzbek Linguistics at Termez State University. She is renowned for her extensive research in Uzbek linguistics and education.

Gulnora Aripova is a professor at the Tashkent Institute of Chemical Technology. Her research focuses on chemical technology, and she has made significant contributions to academia in Uzbekistan.