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

Information Security Framework for Online Language Education Using Differential Privacy and Secure Multi-Party Computation Algorithm

Gulnoza Odilova[1*], Matluba Zaripova[2], Anora Jabbarova[3], Nodira Urinova[4], Muhayyo Davlatova[5], Ibrokhim Sapaev[6], Akbarbek Allashev[7], and Mahina Akhrorova[8]

[1*]Kimyo International University in Tashkent, Tashkent, Uzbekistan. g.odilova@kiut.uz, https://orcid.org/0000-0003-2114-9026

[2]Senior Lecturer, Doctor of Philosophy, Department of Russian Linguistics, Termiz State University, Uzbekistan. zaripovamatlyuba747@gmail.com, https://orcid.org/0000-0002-8490-3412

[3]PhD, Associate Professor, Jizzakh State Pedagogical University, Uzbekistan. jabbarova.anora86@gmail.com, https://orcid.org/0000-0001-6826-2240

[4]Fergana Public Health Medical Institute, Uzbekistan. nodira.urinova.1986@gmail.ru, https://orcid.org/0009-0001-5271-2814

[5]Department of Russian and English Language, Bukhara State Medical Institute, Uzbekistan. davlatova.muhayyo@bsmi.uz, https://orcid.org/0009-0002-0618-7139

[6]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

[7]Lecturer Department of Roman-Germanic Philology, Mamun University, Khiva, Uzbekistan. allashov_akbar@mamunedu.uz, https://orcid.org/0009-0007-6260-2436

[8]PhD, Faculty of Philology, Samarkand State University named after Sharof Rashidov, Uzbekistan. mahinaaxrorova@gmail.com, https://orcid.org/0009-0009-7609-9987

Received: November 14, 2024; Revised: December 19, 2024; Accepted: January 13, 2025; Published: February 28, 2025

Abstract

Online Language Education (OLE) platforms have garnered considerable attention as the need for superior services escalates. Implementing the Mobile Internet of Things (MIoT) encounters numerous obstacles, such as communication security, availability, and scalability. These difficulties directly affect the usage of OLE systems. The constantly changing topology features of MIoT systems complicate the resolution of these difficulties. The research proposes an MIoT paradigm to address these difficulties, efficiently managing the dynamic and developing aspects of network structure, thus improving the system's agility and flexibility. The model can ensure communication confidentiality and security, especially in emergency scenarios for information security. Phishing

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 1 (February), pp. 96-106.
DOI: *10.58346/JISIS.2025.I1.007*

*Corresponding author: Kimyo International University in Tashkent, Tashkent, Uzbekistan.

attempts are now recognized as a significant threat to the security of private information. The present study introduces a novel methodology utilizing Secure Multi-Party Computation (SMPC) to detect phishing assaults on encrypted emails while maintaining data security and privacy. In the framework, the control layer is tasked with calculating routes for Online Educational Devices (OLDs) and directing entries for switching. The controller efficiently orchestrates the system by employing the data gathered from OLDs and amenities for information security. To guarantee the legitimacy and reliability of communications transmitted by OLDs, the research has suggested a novel signature and authentication system utilizing conventional encryption algorithms. The research presents an emergency-handling method incorporating multicast technologies into MIoT, constructing a Steiner Tree among affected nodes to alert OLDs during emergencies swiftly. The security study demonstrates that the MIoT system can guarantee communication safety. An assessment reveals that the method surpasses other current methods.

Keywords: Information Security, Language, Education, Multi-Party Computation.

1 Introduction

Data safety safeguards the company's data from illegal access, publication, or breaches (Rodrigues et al., 2024). Firms must establish robust management procedures that include rules and controls to implement adequate data security (Jeganathan et al., 2024). Technologies offer assistance in safeguarding data assets. A technical solution cannot eradicate the dangers of information leakage, alteration, or breaches for information security. Given the potential for substantial loss, data safety is essential to the operational integrity of most businesses, particularly governmental and public entities, since the monetary and non-financial repercussions are considerably more severe than those faced by other firms (Leitner et al., 2021). Likewise, information leaks or breaches can result in significant losses for educational institutions in Online Language Education (OLE) (Li, 2025) that retain extensive student data within management platforms, administration frameworks, and student websites. Unlawful grade alterations and persistent challenges with registrations or financial processes might compromise the college's trustworthiness and honesty (Tohma & Kutlu, 2020).

The significance of information privacy and security in colleges has been discussed since 1975. Educational institutions (Turnbull et al., 2021) are being attacked for intrusions for two primary reasons. Initially, this is attributable to the substantial computational resources higher education institutions hold. Secondly, they provide public access due to the open availability (Balaban et al., 2025). The communication infrastructures of colleges are accessible not only to faculty and students but to other learners, guests, and academics globally for OLE. Accessibility to the public and the promotion of information sharing must be balanced with the necessity of safeguarding data assets (Joyce & Javidroozi, 2024).

Information security and safeguarding against internal threats are primary considerations for numerous enterprises (Khodjaev et al., 2024). Technology alone cannot ensure safeguarding information against diverse dangers (Sureshkumar et al., 2017). Despite improved technologies, the human aspect continues to pose the primary threat to the integrity of computer security. Many security professionals contend that establishing and enforcing security policies represent the most rational strategy for safeguarding data systems and are essential for a successful security management program. The 'development method' and 'contents' of the safety policy are the two primary factors that dictate the efficacy of the security policy (Mansour, 2024).

There are primarily three categories of Privacy-Preserving (PP) methods: Differential Privacy (DP), Homomorphic Encryption (HE) (Xie et al., 2024), and Secure Multiparty Computation (MPC) (Zhou et

al., 2021) for OLE. Differential privacy strategies guarantee confidentiality by incorporating random noise into personal information. DP is distinguished by little computational cost and elevated efficiency. Preserving accurate statistical data and the considerable reduction in precision constrain its applicability to a certain degree. Another PP technology is HE, which permits specific mathematical operations (e.g., adding and multiplying) to be executed on encrypted information without decoding the initial data. They possess a significant edge in terms of robust security. Executing other intricate operations via HE is challenging compared to linear computations and multiplying. The methods predicated on HE continuously yield inadequate effectiveness and diminished precision. Standard MPC protocols enable n users to jointly compute a specific function F without revealing each participant's private data x. The calculations of MPC are executed using the confidential inputs of several users for OLE. The calculation's outcome is partitioned into n stock allocated to the n users. Each party is unaware of any information regarding the other parties. Its high availability distinguishes MPC. Numerous techniques utilizing MPC technologies for safeguarding sensitive data have been suggested in the research.

The safeguarding of organizational information, which is increasingly kept, analyzed, and transmitted, is becoming more complex and complicated. This is more intricate for knowledge-intensive institutions such as colleges and universities, as their educational and scientific endeavors increasingly rely on the accessibility, reliability, and correctness of digital sources of information. This research examines the formulation of broad outlines and the structural components that a policy should encompass rather than the specifics of security-related rules for information security. The web-based representations of the regulations are evaluated according to the principle of excellent design for OLE.

2 Related Works

CryptoNets was among the initial projects to include homomorphic encryption in the inference phase of Neural Network (NN) algorithms (Pulido-Gaytan et al., 2021). This system utilizes the square function to supplant the conventional activation procedure and a scaling summing function in place of the highest pooling layers, tackling the issue presented by HE’s incapacity to manage non-polynomial and comparative procedures for OLE. CryptoNets attained an accuracy rate for classification of 96.21% on the MNIST database and demonstrated the ability to execute over 52.4k forecasts per hour (Sundara Bala Murugan et al., 2024). The lag for a single forecast was considerable at 560 seconds. The study employed Secret Sharing (SS) technologies to develop an Oblivious NN (ONN) framework. This scheme's safety protocol guarantees the confidentiality of information even in the presence of a semi-honest webserver. The study presented an encrypted NN infer architecture utilizing homomorphic data encryption and distorted circuit technologies. The structure consists of a homomorphic layer, a linear algebra center, and a network interpretation phase. They developed a protocol to transform homomorphic and distorted circuit-encoded data in the system inference stage for OLE. This method obscures additional information regarding the NN, enhances security, and markedly decreases inference time. The investigation established the CryptoDL model to improve the approximations for non-polynomial variables. This framework offers polynomial estimates and hypothetical error limitations for activation equations like Recurrent Learning Unit (ReLU) (Yiğit et al., 2021), Sigmoid, and Tanh, attaining an accurate classification of 99.25% on the MNIST database. The investigation utilized the technique, incorporating a bootstrapping operation to execute the conventional ResNet-20 modeling for information security. They employed the minimax synthesis approach to derive the nonlinear activating operation, attaining ciphertext inference categorization precision nearly equivalent to the performance of the ResNet-20 system training on unencrypted information for information security (Udayakumar et al., 2023).

This enhances the feasibility of applying Fully HE (FHE) to complex PP Machine Learning (ML) (PPML) (Nazarova et al., 2024) systems (Stefanov, 2018). The study presented a model exclusively utilizing the attention process, excluding conventional NN components dependent on loops or convergence, and attained enhanced performance. Scientists have later improved model efficacy by augmenting the number of attention subunits and the size of the concealed layers for OLE. Learned language models have become commonplace, developed using substantial computer resources and vast linguistic datasets. A study devised a PP framework for unorganized text. The study developed SecureNLP, designed to protect machine translation jobs within extended LSTMs, assuring safety within the semi-honest attacker paradigm for information security.

Engagements with the algorithm during operation augment forthcoming datasets. The investigation examined the possibility of adversaries recreating an individual's textual data in federated learning by implementing a one-time key for all member texts. The study presented a naïve Bayes classifier with privacy protections, able to classify garbage in under 23 milliseconds. The study developed a scalable self-supervised learning framework utilizing the differential PP Transformer design that is resilient to adversarial privacy attacks. The research presented Sigma, an approach utilizing function during the preprocessing phase for secure Two-Party (2P) calculation, facilitating secure inferences on GPT modeling with a deduction delay of merely 1.6 seconds for GPT-2 for information security for OLE. The research suggested a token-first packaging approach that reduces the overhead associated with the homomorphic key processing approach in both traditional and digital contexts. The research introduced MPFormer, which replaces the softmax equation and gel activating function—commonly time-intensive in safe inference—with lower-order polynomials and afterward employs distilling of information to mitigate the accuracy reduction resulting from polynomial approximations (Qian et al., 2023). The methodology employs SS to protect both users and simulations. In addition to differing confidentiality, this suggested HE-X architecture utilizes homomorphic security to safeguard the Bert-tiny model's identity while executing approximation calculations on specific activation processes to mitigate the significant processing requirements of universal encryption for OLE.

3 Information Security Framework for OLE

This section outlines the specifics of the suggested structure and explains the planning objectives and the system architecture. The structure of the system is illustrated in Figure 1.

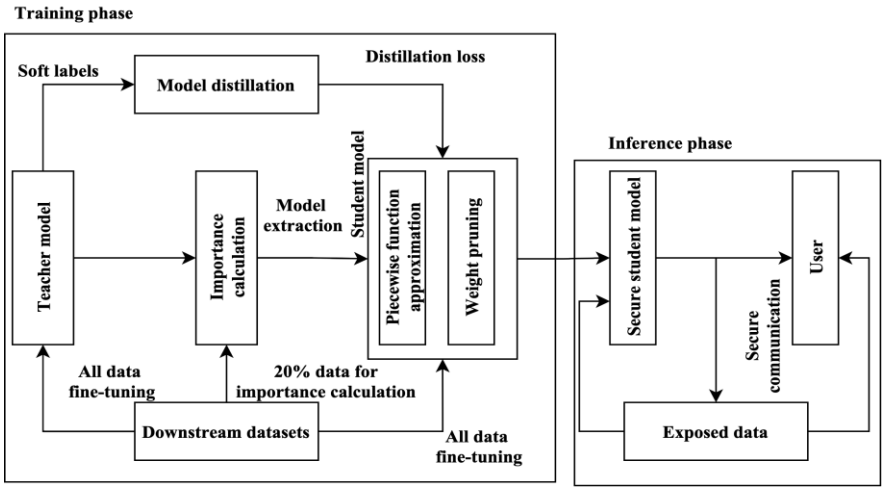

Figure 1: Architecture of the Proposed Model

3.1. Objectives of Design

A PP NN Inference, developed using methods of encryption, must fulfill the subsequent security and performance criteria:

- Accuracy: The forecast outcome should be precise if the customer properly executes the recommended protocol for information security.
- Privacy: The cloud services supplier cannot extract meaningful data upon receiving the consumer's ciphertext. It can only execute specific operations on the ciphertext to fulfill the consumer's objectives for OLE.
- Verification: Upon receipt of the ciphertext from the cloud service supplier, there must be a mechanism to verify the correctness of the result.
- Efficiency: The total time, including dissemination over the channels and inference length, should be considerably shorter than the inference period on the consumer's gadget for OLE.

3.2. System Category and Threat Category

The method involves three distinct entities: the data, model, and computational power suppliers. The cloud supplier hosts the trained algorithm and provides computing capabilities. The framework presents a computational power supplier positioned among the information and model suppliers for information security. Employing an SS mechanism for safe inference necessitates segmenting and distributing specific model variables to the client by exchanging confidential information with a cloud service for OLE. As a result, users bear a share of the cognitive and communicational burden. In this approach, customers must exchange information just once with the computing resource supplier, who assumes the subsequent mathematical and communicational duties in conjunction with the model suppliers for information security.

3.3. Model

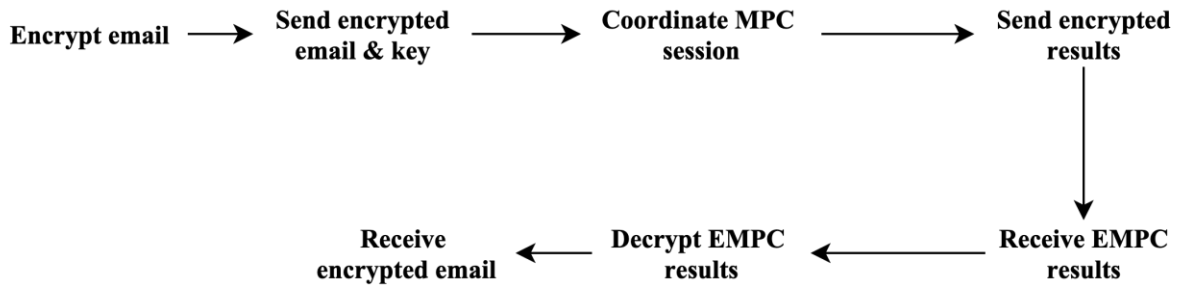

Figure 2: Phishing Link Detection Process

As seen in Figure 2, the suggested system consists of three essential entities: the sender, the recipients, and the web server. Each entity has a distinct function in ensuring email messages are handled securely and privately. The original sender initiates transmitting the encoded email message to the website, which employs the Secure MPC (SMPC) method to detect phishing Uniform Resource Locators (URLs) within the encoded email. Upon identification, the server sends the encoded outputs of the SMPC method to both the sender and the recipient. The SMPC partners decode the outputs and, based on their choice, either block or permit email transmission for information security.

The sender proactively ensures the privacy of the e-mail content during its transmission. The process commences by encrypting what is in the email using a method referred to as Partially Homomorphic for OLE. The recipient decrypts and processes the output while maintaining the private nature of the email. Its function commences upon receiving the encrypted email from the website, which includes a flag indicating the presence of a malicious link. It determines whether to block or transmit the email based on this flag for OLE. Communication among the SMPC participants is encrypted. This renowned secure method guarantees that transferred traffic is fully protected while preventing illicit access.

3.4. SMPC

The SMPC element (Figure 3) handles email, ensuring data anonymity and security. This component is divided into three different sub-models:

- Obtaining the content of the email: The server accepts the email provided via the HyperText Transfer Protocol Secure (HTTPS) method to ensure data security and integrity.
- SMPC Session Configuration: The server performs data processing without decryption.

Detection of phishing URLs by employing the suitable SMPC method, the server attains OLE identification. Depending on the adaptation algorithm, it hires feature mappings or an unsupervised section.

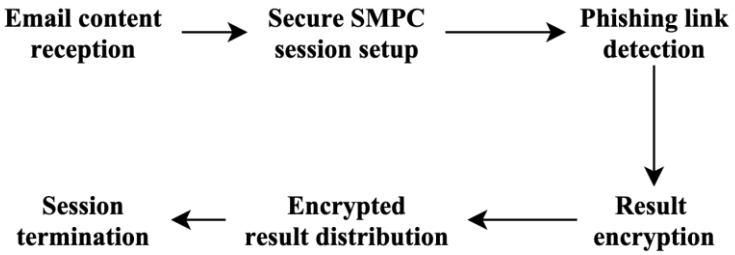

Figure 3: SMPC Module

3.5. Output Encrypting

- The server obtains the results after the execution of the SMPC method.
- It adds a signal indicating whether the email contains a phishing assault.
- The server transmits encoded findings to the recipient with utmost security.
- This maintains the confidentiality of the outputs and guarantees that they are accessible solely to authorized parties.
- The server terminates the secure SMPC session after broadcasting its results to prevent data compromise.

4 Results

The Gated Recurrent Unit (GRU) network's activity focuses on securely computing the sigmoid and tanh values. Initially, the research executed the three fundamental protocols: SecuredSigmoid, SecuredTanh1, and SecuredTanh2 within a 2P framework. Figure 4 illustrates the execution time and the communication aspects of different systems for information security. The communication overhead denotes the communication necessitated by all parties during the implementation of a protocol. In the

three-party (3P) context, the research executed the fundamental protocols by utilizing the duplicated sharing of secrets method within the architecture of OLE. Reproduced SS is an additive inside a 3P framework. The repeated secret-sharing mechanism facilitates expedited multiplication operations and reduces communication, rendering these methods more effective in a 3P context than a 2P one.

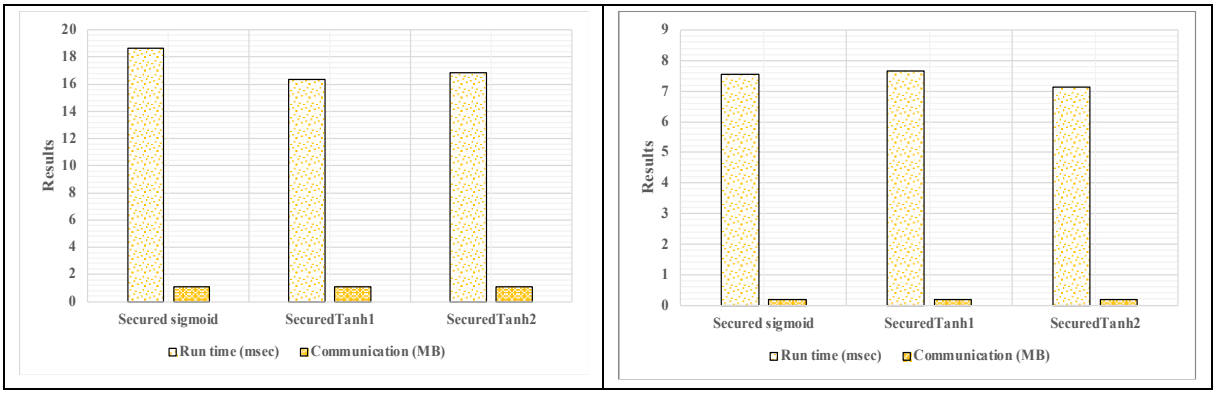

Figure 4: Runtime (RT) and Communication Expenses (CE) Analysis (a) 2P (b) 3P Settings

Figure 4 illustrates the RT and interaction of these fundamental protocols in a 3P context. The execution time of these fundamental protocols is in the millisecond region. The RT is consistently under 7.2 ms in the 3P configuration for OLE. The three fundamental protocols necessitate an equivalent level of interaction for every operation. The reason is that both Secured Sigmoid and Secured Tanh necessitate an identical quantity of multiplication activities, and the communication needed for these multiplication processes remains constant for information security.

The learning process of the attention-based GRU network utilizes the TensorFlow framework. The input text series T has a maximum size of 95 characters. Initially, the research evaluated the efficiency of Secured GRU in a 2P configuration for OLE. To facilitate comparison and applicability, the study assessed the RT and CE of Secure GRU with varying input sequence sizes. Figure 5 presents the RT and CE that fluctuate with the size of the input sequences. To enhance RT efficiency and reduce CE, the research created Secured GRU utilizing the replication method within a 3P framework.

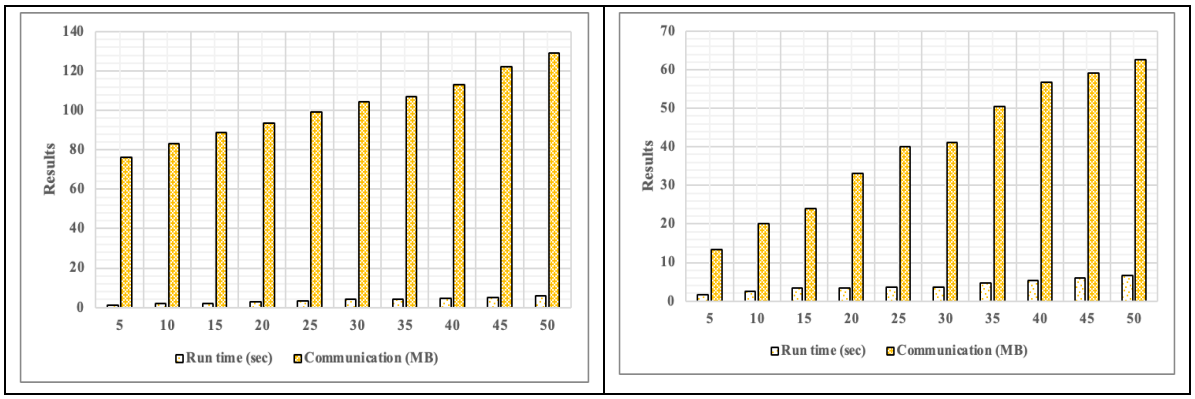

Figure 5: RT and CE Analysis of Secured-GRU (a) 2P (b) 3P Settings

Figure 6 demonstrates that the RT and CE of SecuredGRU increase linearly with sequence size in both the 2P and 3P configurations for information security. The repeated SS method substantially decreases RT and CE in a 3P configuration compared to a 2P configuration, particularly for CE.

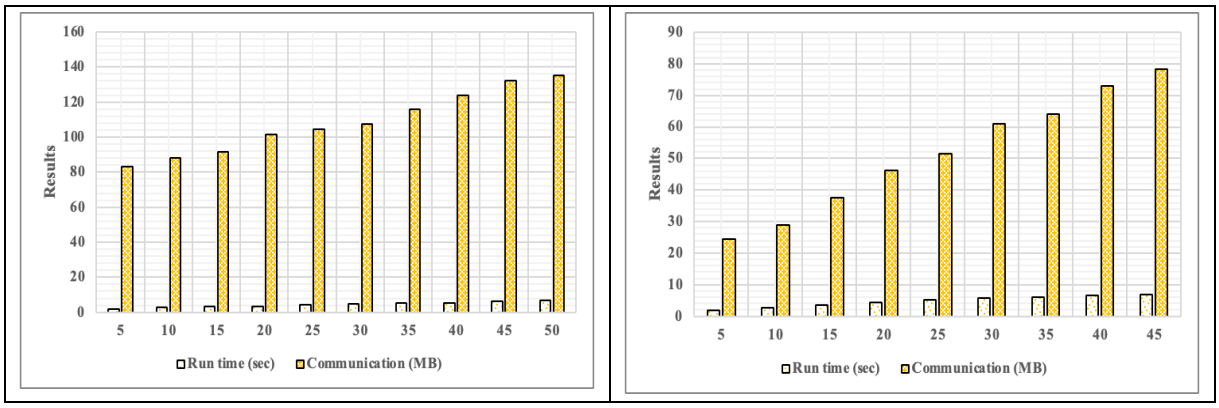

Figure 6: RT and CE Analysis of Secured- Reservoir Computing (RC) (a) 2P (b) 3P Settings

The research compared the experimental outcomes of SecuredRC in the 2P and 3P configurations for information security. The RT and CE of SecuredRC increase linearly with the series size for OLE. The interaction expenses of security in the 3P configuration are diminished by a factor of ten compared to those in the 2P configuration.

5 Conclusion

This study presents a safe communication framework utilizing a multicast method within MIoT. Initially, the research developed a multicast tree system. This method employs multicast methods to rapidly create a multicast tree across impacted OLD following disasters for OLE. A flexible signature authentication approach is developed to secure MPC, ensuring compliance with safety standards like confidentiality, privacy conservation, and tracing for information security. The system facilitates batch authentication, hence optimizing resource utilization. The safety proof performed within the random oracle paradigm indicates that the suggested method fulfills the security criteria for secure interaction in MloT for OLE. The efficacy evaluation of the method demonstrates its superiority in RT and CE for information security.

The system fails to account for the actual distribution of OLE, resulting in suboptimal efficiency. In the future, the research will concentrate on categorizing OLD according to the suggested system, enhancing the management of OLD in device-intensive regions.

References

[1] Balaban, B., Magara, S. S., Yilgor, C., Yucekul, A., Obeid, I., Pizones, J., ... & European Spine Study Group. (2025). Privacy-Preserving Machine Learning (PPML) Inference for Clinically Actionable Models. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3540261

[2] Jeganathan, S., Lakshminarayanan, A. R., Parthasarathy, S., Khan, A. A. A., & Sathick, K. J. (2024). OptCatB: Optuna Hyperparameter Optimization Model to Forecast the Educational Proficiency of Immigrant Students based on CatBoost Regression. *Journal of Internet Services and Information Security*, *14*(2), 111-132. https://doi.org/10.58346/JISIS.2024.I2.008

[3] Joyce, A., & Javidroozi, V. (2024). Smart city development: Data sharing vs. data protection legislations. *Cities*, *148*, 104859. https://doi.org/10.1016/j.cities.2024.104859

[4] Khodjaev, N., Boymuradov, S., Jalolova, S., Zhaparkulov, A., Dostova, S., Muhammadiyev, F., Abdullayeva, C., & Zokirov, K. (2024). Assessing the effectiveness of aquatic education program in promoting environmental awareness among school children. *International Journal*

of Aquatic Research and Environmental Studies, *4*(S1), 33-38. https://doi.org/10.70102/IJARES/V4S1/6

[5] Leitner, M., Frank, M., Langner, G., Landauer, M., Skopik, F., Smith, P., ... & Warum, M. (2021). Enabling exercises, education and research with a comprehensive cyber range. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *12*(4), 37-61. https://doi.org/10.22667/JOWUA.2021.12.31.037

[6] Li, Y. (2025). The impact of teacher support on OLE in RFL learners: The chain mediating roles of classroom enjoyment and motivation. *Acta Psychologica*, *252*, 104677. https://doi.org/10.1016/j.actpsy.2024.104677

[7] Mansour, R. (2024). A Conceptual Framework for Team Personality Layout, Operational, and Visionary Management in Online Teams. *Global Perspectives in Management*, *2*(4), 1-7.

[8] Nazarova, S., Askarov, M., Karimov, N., Madraimov, A., Muminov, A., Abirov, V., & Shosaidov, A. (2024). The Role of Online Libraries in Advancing the Study of Uzbek Culture. *Indian Journal of Information Sources and Services, 14*(3), 207–215. https://doi.org/10.51983/ijiss-2024.14.3.26

[9] Pulido-Gaytan, B., Tchernykh, A., Cortés-Mendoza, J. M., Babenko, M., Radchenko, G., Avetisyan, A., & Drozdov, A. Y. (2021). Privacy-preserving neural networks with homomorphic encryption: C hallenges and opportunities. *Peer-to-Peer Networking and Applications*, *14*(3), 1666-1691. https://doi.org/10.1007/s12083-021-01076-8

[10] Qian, J., Zhang, P., Zhu, H., Liu, M., Wang, J., & Ma, X. (2023). Lhdnn: Maintaining high precision and low latency inference of deep neural networks on encrypted data. *Applied Sciences*, *13*(8), 4815. https://doi.org/10.3390/app13084815

[11] Rodrigues, G. A. P., Serrano, A. L. M., Vergara, G. F., Albuquerque, R. D. O., & Nze, G. D. A. (2024). Impact, compliance, and countermeasures in relation to data breaches in publicly traded US companies. *Future Internet*, *16*(6), 201. https://doi.org/10.3390/fi16060201

[12] Stefanov, V. (2018). Communication Technology-led Development in Kenya and Sub-Saharan Africa's Education Systems: A Cross Sectional Study. *International Journal of Communication and Computer Technologies (IJCCTS)*, *6*(2), 1-5.

[13] Sundara Bala Murugan, P., Ganesan, A., Paranthaman, P., & Aruna, V. (2024). Feasibility Design and Analysis of Process-aware Accounting Information System for Business Management. *Indian Journal of Information Sources and Services, 14*(2), 56–62. https://doi.org/10.51983/ijiss-2024.14.2.09

[14] Sureshkumar, T., Lingaraj, M., & Anand, B. (2017). A Review on Network Security Mechanisms for Policy Analysis. *International Journal of Advances in Engineering and Emerging Technology*, *8*(3), 1-8.

[15] Tohma, K., & Kutlu, Y. (2020). Challenges Encountered in Turkish Natural Language Processing Studies. *Natural and Engineering Sciences, 5*(3), 204-211. https://doi.org/10.28978/nesciences.833188

[16] Turnbull, D., Chugh, R., & Luck, J. (2021). Transitioning to E-Learning during the COVID-19 pandemic: How have Higher Education Institutions responded to the challenge?. *Education and Information Technologies*, *26*(5), 6401-6419. https://doi.org/10.1007/s10639-021-10633-w

[17] Udayakumar, R., Joshi, A., Boomiga, S. S., & Sugumar, R. (2023). Deep Fraud Net: A Deep Learning Approach for Cyber Security and Financial Fraud Detection and Classification. *Journal of Internet Services and Information Security, 13*(4), 138-157.

[18] Xie, Q., Jiang, S., Jiang, L., Huang, Y., Zhao, Z., Khan, S., ... & Wu, K. (2024). Efficiency optimization techniques in privacy-preserving federated learning with homomorphic encryption: A brief survey. *IEEE Internet of Things Journal*, *11*(14), 24569-24580. https://doi.org/10.1109/JIOT.2024.3382875

[19] Yiğit, E., Özkaya, U., Öztürk, Ş., Singh, D., & Gritli, H. (2021). Automatic detection of power quality disturbance using convolutional neural network structure with gated recurrent unit. *Mobile Information Systems*, *2021*(1), 7917500. https://doi.org/10.1155/2021/7917500
[20] Zhou, J., Feng, Y., Wang, Z., & Guo, D. (2021). Using secure multi-party computation to protect privacy on a permissioned blockchain. *Sensors*, *21*(4), 1540. https://doi.org/10.3390/s21041540

Authors Biography

Gulnoza Odilova is an accomplished academic at Kimyo International University in Tashkent, Uzbekistan. Her research focuses on interdisciplinary studies, contributing significantly to academic publications and conferences.

Matluba Zaripova is a Doctor of Philosophy and Senior Lecturer at the Department of Russian Linguistics, Termez State University. She is recognized for her contributions to linguistics and higher education.

Anora Jabbarova is a PhD holder and Associate Professor at Jizzakh State Pedagogical University. She specializes in education and linguistics and is actively involved in research and mentorship.

Nodira Urinova is an academic affiliated with the Fergana Public Health Medical Institute. Her work focuses on public health and medical research, with contributions to several academic forums.

Muhayyo Davlatova is a lecturer at the Department of Russian and English Language, Bukhara State Medical Institute. She is known for her research in linguistics and multilingual education.

Ibrokhim Sapaev is a multidisciplinary researcher serving as the Head of the Department of "Physics and Chemistry" at the Tashkent Institute of Irrigation and Agricultural Mechanization Engineers. His research encompasses physics and applied sciences, contributing to academic excellence across multiple institutions.

Akbarbek Allashev is a lecturer in the Department of Roman-Germanic Philology at Mamun University, Khiva. His expertise lies in linguistics and philology, with a focus on language education and research.

Mahina Akhrorova holds a PhD and serves in the Faculty of Philology at Samarkand State University named after Sharof Rashidov. Her research interests include philology and language studies.