Taylor & Francis
Taylor & Francis Group

Applied Artificial Intelligence
An International Journal

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uaai20

Zero-Knowledge Proof Intelligent Recommendation System to Protect Students' Data Privacy in the Digital Age

Wenjing Yin

To cite this article: Wenjing Yin (2023) Zero-Knowledge Proof Intelligent Recommendation System to Protect Students' Data Privacy in the Digital Age, Applied Artificial Intelligence, 37:1, 2222495, DOI: 10.1080/08839514.2023.2222495

To link to this article: https://doi.org/10.1080/08839514.2023.2222495

Published online: 13 Jun 2023.

APPLIED ARTIFICIAL INTELLIGENCE
2023, VOL. 37, NO. 1, e2222495 (2099 pages)
https://doi.org/10.1080/08839514.2023.2222495

Taylor & Francis
Taylor & Francis Group

Zero-Knowledge Proof Intelligent Recommendation System to Protect Students' Data Privacy in the Digital Age

Wenjing Yin

Zhengzhou Preschool Education College, Preschool Education Institute, Zhengzhou, China

ABSTRACT

The rapid digital revolution in recent decades has resulted in an overwhelming amount of information, particularly in the realm of modern education systems and related materials. This phenomenon, often referred to as information overload, necessitates the development of educational systems that can effectively search, classify, and categorize this vast amount of available information. Of utmost importance for such educational information systems is the safeguarding of personal data, which refers to information that can identify an individual or their family. School records, for example, contain various types of personal data such as the individual's name, address, contact details, disciplinary history, as well as their grades and progress checks. Even if individuals choose to make this data public, it remains inherently personal. Another category of data involves more sensitive topics such as student biometrics (e.g. fingerprints, photographs), religious beliefs, health information (e.g. allergies), or dietary restrictions, which may imply religious or health-related aspects. Processing data in this category can pose risks to individuals; hence, strict rules and appropriate consent are necessary to ensure their protection. To address these challenges, this research paper proposes a zero-knowledge proof intelligent recommendation system designed to protect students' data privacy in the digital age. The proposed method incorporates an Intelligent Recommendation System (IRS) that utilizes an optimized version of the Matrix Factorization technique, calculated as an Eulerian Walk chart. Furthermore, the Schnorr Zero-Knowledge Proof format, based on the discrete logarithm problem, ensures the privacy of personal data during message exchange between educational entities.

ARTICLE HISTORY
Received 5 May 2023
Revised 1 June 2023
Accepted 4 June 2023

Introduction

One of the first consequences of the coronavirus, inextricably linked to the digital gigantism of recent years, has already made a strong appearance in modern education (Zheng, Yin, and Demertzis 2022). For some time now, educational institutions of all levels have been incorporating digital

CONTACT Wenjing Yin 2014006@zzpec.edu.cn Zhengzhou Preschool Education College, Preschool Education Institute, Zhengzhou 450000, China

technologies into their operation due to the spread of the coronavirus by the state measures for the protection of public health that have been taken (Ahmad 2020; Chigada and Madzinga 2021). As a result, many of the courses are now offered remotely and online, as there has been a clear upgrade of technology services during incarceration and a considerable amount of time to adapt to the new data (Hatzivasilis et al. 2020).

In the face of the new educational reality, the challenges that arise are many: both for the teachers, who are called to become thoroughly acquainted with this situation, and for the learners, who are called to be taught with new methods and means (Zoolfakar and Sulaiman 2009). Undoubtedly, the standard component is the expectation and the goal of providing quality and modern education for the benefit of society (Chang 2021).

Online education cannot function without ensuring the safety of the personal information of everyone who has anything to do with its delivery. The most critical question is whether or not the confidentiality of students and teachers is preserved. The usage of cameras during online learning, the recording and uploading of educational lectures, and the best approach to assure the reliability and validity of the assessment process by leveraging different kinds of technology are some of the challenges that emerge here (Wang et al. 2020; Zhang and Demertzis 2022).

Using technological tools to assess students always involves processing and collecting personally identifiable information as the first step. For data processing to be lawful, it is necessary to comply with all relevant principles and conditions. The institution must confirm that the information they gather on their trainees and instructors is legal and will be safeguarded in compliance with applicable state and federal regulations (Wang and Demertzis 2022).

More specifically, each educational institution must inform the stakeholders about how this processing is done, what information is collected, and with what technological tools. The purpose of data processing is essential as it serves as a criterion for further legitimacy of processing. At the same time, the subject should be guaranteed the right to access this personal information (Chang 2021). The data storage period must be defined and known to individuals. Accordingly, their deletion should take place if the specified purpose disappears. The general framework for personal processing data is analyzed in the data protection policy of the educational institution, which must be accessible to the subjects. However, the new conditions created to increase the degree of security required, primarily when, for example, a camera is used, and additional information is collected, such as the image of the face, the voice, and others (Tahiri, Bennani, and Idrissi 2016).

Especially in terms of using the camera and videotaping the lessons, some critical points need to be emphasized. Initially, the video recording is considered legitimate as it is provided per the directive of the Agency for Quality Assurance and Certification of educational services and if this is

subject to the relevant provisions of the broader law on personal data protection. Its purpose is to verify the quality of teaching (Perez et al. 2017; Wehrmann et al. 2018). Before lectures may be posted on the educational institution's electronic platform, they must first be approved by the teacher in question and the students who will be participating. (Uploading the lecture by the instructor should be preferred for the teacher's overall quality of education, particularly if the students agree; this is primarily due to objective barriers such as incapacity to visit professors' offices or the school.) As a result, both teachers and students cannot utilize it, albeit it is highly recommended that they do so to ensure the legitimacy of the material conveyed in the class. However, unless specifically instructed otherwise, the participant is free to use a camera at any moment throughout the experiment (He et al. 2017). Consent should be given freely, explicitly, and unconditionally, as provided by law. Withdrawal of support can be made at any time. This practically means that it will not occur if a student does not wish to post the lecture on the electronic platform. An alternative may be suggested, provided the camera is used, and the other students agree, not to be used by the dissenter or to delete the material where the student in question appears or is heard. Of course, in case the lecture is posted, it should be emphasized that further posting on other media or its notification to unauthorized persons is prohibited (Zhang and Demertzis 2022).

In addition, the student evaluation based on their presence in the videotaped lectures should be prevented as this leads to the compilation of a profile. Consequently, the student's evaluation should be a function of additional factors, such as their performance in assignments, their previous presence in the classroom, and other criteria (Hassanpour et al. 2019; Murphy 2012).

How the examination period may be conducted utilizing technology methods, notably video monitoring of the student, is a topic that is of considerable interest. It is not assured that any gaps or deficiencies will be avoided if there is no physical presence in a classroom or other instructional space. Nevertheless, there is an absolute need to respect people's right to privacy. To ensure the legitimacy of the process, the use of dependable technological tools and the student's free and informed consent, an educational institution must ensure that it uses a camera as an examination method. This is especially important if the institution chooses to use this method.

Regarding the last concern, it is essential to point out that the learner's permission is seen as being free and lawful when they are presented with alternative testing techniques that are equal and similar and do not have any adverse effect on their grade. However, the consent gained is void if given a lower rate or suffered some other harm. If this is not possible, an alternative method is advised, such as if a video presence examination is refused, to guarantee the procedure's dependability and quality (Lin et al. 2018).

Also, in case video presence is chosen as a means of the final examination, the minimum data for this purpose must be collected, and the protection of the rights of third parties must be prevented, for example, in the case where information may be disclosed, directly or indirectly for members of the wider family environment or other sensitive data. For this reason, the conduct of an impact assessment by the educational organization on the potential risks of data processing in such a case, which is also required by law, is even more critical (Andergassen et al. 2015; Gabay, Akkaya, and Cebe 2020).

In conclusion, the picture that has been formed in education in recent years is considered, if not unprecedented, undoubtedly provocative. Stakeholders are called upon to take on even greater responsibilities for the benefit of society. Given that there is no absolute level of security on the internet, what is required is the minimization of risks; the problems and concerns that arise for the protection of privacy concern everyone and need to be organized and coordinated action (Lin et al. 2018; Zoolfakar and Sulaiman 2009).

Significant efforts have been made to implement advanced systems, which add technological solutions to the privacy protection of modern educational systems. A critical analysis of the most recent respective research efforts is presented in the following section.

Literature Review

The literature on Artificial Intelligence (AI) research in e-learning has grown in recent years, owing to the tremendous potential of AI in the educational process, particularly personalization (Li et al. 2021; Pasquet et al. 2014). Most experts agree that artificial intelligence in education, especially e-learning, offers enormous theoretical and pedagogical promise. However, before completely incorporating technology into educational processes, it is necessary to establish a critical posture. To avoid automated procedures and machine learning, testing and evaluating AI in educational methods is essential.

To increase the accessibility and efficacy of the cognition of intelligent education, Lin et al (Lin et al. 2018), suggested a unique recommendation method for course choice in the field of data integration in regional institutions. They first gathered the course registration data set for a particular group of students to develop this method. In their framework, the Sparse Linear Method was added to get skilled of courses that would be suitable for the students. An approximation term was constructed and used as the optimization technique by examining the course elements in the existing classification model (Zhang and Demertzis 2022). To assess the strategy's effectiveness, studies were conducted on cutting-edge methodologies and their style. They also evaluated our method's effectiveness using the reliability of various courses and course themes, and the results once more validate the best practices of their strategy (Daras et al. 2020).

Despite the openness and transparency of blockchain, there are still some privacy concerns when implementing transactions. To highlight security issues and obstacles, Sun et al (Sun et al. 2021), thoroughly assessed Zero-Knowledge Proof in the chain ecosystem. As a result, they researched the application of ZKP in the context of blockchain. They offered an introduction to blockchain and covered ZKP frameworks, models, and applications, as well as a framework for ZKP in a blockchain setting (Gabay, Akkaya, and Cebe 2020). They then determined some potential issues, and future study focuses.

A method for guaranteeing the confidentiality of prosumer data was put out by Pop et al. (Pop et al. 2020). On top of the open blockchain, they provided a decentralized application of demand policy responses that uses smart contracts to verify participant behavior inside the program and zero-knowledge proofs to protect the privacy of prosumers' energy data. Energy data from consumers was kept private. A zero-knowledge guarantee that the prosumer generated is held on the blockchain, enabling the development of functions to verify alternate points from the request and resolve the prosumer's activities. The results of the solution evaluation are encouraging in terms of protecting the confidentiality of prosumer power data stored in the open blockchain and spotting any data anomalies. The findings indicated that their approach had promise for protecting the privacy of prosumer-monitored energy data while enabling aggregators to carry out validations and spot potential variances from the flexibility request. They also attempted to make it possible for aggregators to verify and spot potential instances of flexibility tampering with prosumer-registered data.

Using distributed applications made possible by Blockchain and smart contracts, Gabay et al (Gabay, Akkaya, and Cebe 2020). adaptation of zero-knowledge proofs to Blockchain enables privacy-preserving authentication while doing away with the requirement for a central authority to handle the issue. They presented two methods to achieve anonymous authentication, one utilizing the Pederson Commitment technique and the other using a token-based system. They also provided a methodology for the entire procedure, which covered processes for scheduling and charging. The analysis of the suggested methods revealed that the waste of this procedure is manageable enough to allow linked electric vehicles to operate in real-time charging. By fusing the idea of zero-knowledge evidence and Chain smart contracts, they presented a framework to protect EVs' privacy during the charging process. They demonstrated through security analysis that their strategy did not expose any information to the relevant parties. The outcomes showed that the total overhead in terms of costs and Cryptocurrency cost is reasonable for use in practical applications. However, the Pederson technique performs better than the token-based strategy in money terms overhead.

To address the problems with data integrity and privacy preservation in blockchain-based transport systems, Li et al (Wanxin Li et al. 2020), presented

a modular and location-aware architecture. Their solution relied on a gateway mechanism using zero-knowledge range proof to ensure that linked autos moved across blockchain networks without revealing personal information. The non-interactive zero-knowledge range evidence (ZKRP) protocol was combined with a modular blockchain and authorization. They used the Hyperledger Caliper measurement tool to measure the benchmarks for the decentralized network, such as session latency, bandwidth, and success rate. They evaluated the proof-producing and verifying times for the ZKRP scheme under various conditions. The findings show that their method of distributed traffic control was realistic and practicable.

Given the impossibility of implementing a complete solution for protecting personal rights and especially information containing sensitive personal information, this research effort presents an advanced zero-knowledge proof intelligent recommendation system to protect students' data privacy in the digital age. The proposed system initially uses an IRS, a hybrid format combining Matrix Factorization techniques as part of an Eulerian Walk chart. Schnorr's digital key signature format is also used to ensure the privacy of personal information when exchanging messages between educational entities.

Intelligent Recommendation System

The proposed IRS (Lin et al. 2018) is based on the application logic of recommendation systems. A referral system is a subset of an information filtering system that seeks to predict user preferences for an item based on relevant personal knowledge filtering (Abdi, Okeyo, and Mwangi 2018). In particular, the proposed recommendation system is based on the creation of an algorithmic information filtering system, which seeks to predict the "rating" or "preference" that a security expert would give to an element or action of the educational environment based on the ideal weighting of protection of users' data (Wan, Zhou, and Ren 2022). The predictions/recommendations are made after analyzing the behavioral characteristics and relevant information about the user experience, its role in the system, and its interaction with the service. Prediction outcomes may be improved by assigning various adjustment weights to latent components depending on data popularity and user activity, particularly the Matrix Factorization approach (Abdi, Okeyo, and Mwangi 2018) is used as a category of cooperative filtering algorithms to factorize tables, decomposing the user-object interaction table into the product of two orthogonal tables of lower dimensions.

The available methods for making recommendations use feature matrices and the whole network for convolutions. On the other hand, the suggested method selects neighboring nodes in a graph. By dynamically constructing computational networks, it is possible to function with local convolutions more effectively. The application of convolutions to a node's whole

neighborhood will generate a massive computational network. Simulating a random walk is one method that is used in the construction of convolutional networks. This method is used to choose frequently seen information as the crucial region. The k-hop community of the node is combed through for new information, which is then used to update the node representations. Due to the frequent overlap of k-hop zones, repeated computation is necessary. Consequently, the proposed method maps all of the nodes without repeatedly performing calculations, link the lower-level nodes to the important upper-level nodes, and locates the embeddings of the upper-level nodes in each aggregation step.

The above discusses different approaches to making recommendations and highlights a suggested method that utilizes neighboring nodes in a graph. Specifically:

(1) Traditional recommendation methods use feature matrices and the entire network for convolutions: In traditional recommendation systems, feature matrices are commonly used to represent user-item interactions or other relevant features. These matrices are then used in convolutional operations, which typically involve considering the entire network or dataset during computation.
(2) The suggested method employs local convolutions using neighboring nodes in a graph: In contrast to the traditional approach, the suggested method focuses on utilizing the graph structure of the data. Instead of considering the entire network, it selects neighboring nodes to perform convolutions. This allows for more localized and efficient computations.
(3) Dynamic construction of computational networks: The suggested method dynamically constructs computational networks, meaning that the network structure is generated or adapted based on the specific task or data. This enables more effective utilization of local convolutions and can lead to improved recommendation performance.
(4) Simulating random walks for constructing convolutional networks: Random walk simulation is one approach used in constructing convolutional networks within the suggested method. By simulating random walks, the method identifies frequently visited nodes or regions, considering them as crucial areas for information retrieval. The k-hop community of a node (a set of nodes reachable within k steps) is explored for new information, which is then used to update node representations.
(5) Repeated computation and overlap of k-hop zones: Since k-hop zones of different nodes often overlap, there is a need for repeated computation when considering multiple nodes. This can result in computational inefficiency.

(6) Proposed method: The proposed method aims to address the inefficiency caused by repeated computation. It achieves this by mapping all nodes without redundancy, linking lower-level nodes to important upper-level nodes, and locating embeddings (representations) of upper-level nodes in each aggregation step. This approach minimizes redundant calculations while preserving important information from the graph structure.

The use of feature matrices and whole-network convolutions in traditional recommendation methods, contrasts it with the suggested method that employs local convolutions using neighboring nodes in a graph, and highlights the benefits of dynamically constructing computational networks. It also mentions the use of random walk simulation for constructing convolutional networks and the proposed method's approach to reducing redundant computations while maintaining important information.

By a broader logic, the problem of assigning appropriate recommendations to ensure the privacy of those involved in a system in this study is implemented as a system of graphs. In discrete mathematics, a chart is an abstract representation of a set of elements, where several pairs of elements are linked together by bonds. The interconnected elements are represented by mathematical concepts called vertices, while the bonds that connect the pairs of vertices are called edges (Yan et al. 2016). The edges can be directed (asymmetric) or non-directed (symmetrical). A trace in a graph is a sequence of alternating nodes and edges such that its first and last element is a node, while no edge is repeated (i.e., it does not appear in the sequence more than once) (Wanxin Li et al. 2020). If the first and last elements of the trace are identical, then we have a circuit. A trace between two different nodes u and v of a graph is the Euler trace; if it contains all the edges of the graph while if the circuit includes all its edges, then we have an Euler circuit (Sun et al. 2021).

So, we can model the problem of privacy recommendations through a graph where the correlations of the stakeholders correspond to nodes in the graph, and two nodes are adjacent if the edges joining the respective recommendations do not join the third recommendation. So, from this point of view, the problem is reduced to the following graph-theoretical problem: In a coherent graph G, find a minimum closed walk containing all the edges of the graph's G (Eulerian walk) (Lam et al. 2015; Menci 2002; Ugurlu and Kawamura 2010).

To solve this technique, we assume the coherent graph G representing the issue to be an Euler graph, giving us an algorithm right away. To find an Euler circuit of G, start and terminate the Euler walk at the beginning and destination nodes w. If G is not an Euler graph, we use an alternate solution approach, detailed below (Yan et al. 2016).

A two-partition of the set $V_{\text{odd}}(G) = \{u_1, u_2, \ldots, u_{2k}\}, k \geq 1$ (the set of nodes of odd degree G) is a partition of k into subsets of the two elements. For a two-member partitioning (Hassanpour et al. 2019):

$$\pi = \{(x_1, y_1), (x_2, y_2), \ldots, (x_k, y_k)\} \tag{1}$$

We define the distance $d(\pi)$ of π as the sum of the distances of its members in the graph G, i.e.:

$$d(\pi) = \sum_{i=1}^{k} d(x_i, y_i) \tag{2}$$

Let $\mu(G) = min\{d(\pi)\}$, for each π of G (the minimum is calculated on all two-partition π of the set $V_{\text{odd}}(G) = \{u_1, u_2, \ldots, u_{2k}\}, k \geq 1$, It is evident that if G is an Euler graph, $V_{odd}(G) = \emptyset$ holds, and then we define $m(G) = 0$.

But because we are interested in studying the mechanism for assigning privacy recommendations to multivariate scenario processes, the problem lies in finding a Hamiltonian minimum weight cycle in the (complete) graph G. In this case, an obvious algorithm for solving the problem requires weight calculation of $(n-1)!/2$ Hamilton cycles of graph G. The time complexity of such an algorithm is exponential, and therefore the algorithm is inefficient. An alternative approach is to try to solve the optimization problem (Gong, Zhao, and Lu 2007; Yamamoto, Uchitane, and Hatanaka 2012):

$$\underset{z^*}{\text{argmin}}\left\{\| G(z^*) - x \|^2\right\} \tag{3}$$

To solve this optimization problem, we propose a new inversion method that uses Discriminator to solve the minimization problem in a different representation space. Specifically, we start with a random latent variable z and a given actual composition x. We denote by D^0 the network of the separator just before the level of attention, and we get the expressions $D^0(G(z))xandD^0(x)$. The proposed algorithm allows us to minimize the following quantity (Cao et al. 2008; Xue, Zhang, and Neri 2021):

$$\| \left(D^0(G(z)) - D^0(x)\right) \cdot S' \|^2 \tag{4}$$

where S' is a scaled version of the node significance map in the dimensions of $D^0(x)$. In this case, one solution is to calculate the above equation separately for each node and then add the other losses. In this case, the new loss function is given by the following equation:

$$\sum_i \| \left(D^0(G(z)) - D^0(x)\right) \cdot S_i^{'} \|^2 \tag{5}$$

Generalizing the problem of deciding on the ratio of graph density, given those dense models produce sparse maps even under very loose case data, we

provide a limit to the number of non-sparse positions in the algorithm in which Input data are samples (not necessarily independent) with the same mean and variance. To do this, we will need the result on the rarity of the probabilistic distributions obtained from the graph, which in a general classification hypothesis can be determined as follows (Wei Li, Xia, and Huang 2020; Murphy 2012; Rafiei and Adeli 2017):

$$\text{If } n\in \geq 1 \text{and} k \leq \frac{1+(n+1)\ln^2(n\in)}{1+\ln^2(n\in)} \text{then} E\left(\frac{e^{X_{k:n}}}{\sum_{i=1}^{n} e^{X_{i:n}}}\right) \leq \in \tag{6}$$

the upper limit should be calculated for the function:

$$E\left(\frac{e^{X_{k:n}}}{\sum_{i=1}^{n} e^{X_{i:n}}}\right) \tag{7}$$

Thus, based on Jensen inequality, the definition of the convex function, i.e.

$$E\left(\frac{e^{X_{k:n}}}{\sum_{i=1}^{n} e^{X_i}}\right) \leq \frac{e^{E(X_{k:n})}}{\sum_{i=1}^{n} e^{E(X_i)}} \tag{8}$$

Function which is generalized as:

$$\frac{e^{E(X_{k:n})}}{\sum_{i=1}^{n} e^{E(X_i)}} \leq \frac{e^{\mu+\sigma\sqrt{\frac{k-1}{n-k+1}}}}{\sum_{i=1}^{n} e^{E(X_i)}} = \frac{e^{\mu+\sigma\sqrt{\frac{k-1}{n-k+1}}}}{ne^{\mu}} \tag{9}$$

And applying $\mu = 0$ and $\sigma^2 = 1$, we have:

$$E\left(\frac{e^{X_{k:n}}}{\sum_{i=1}^{n} e^{X_{i:n}}}\right) \leq \frac{e^{\sqrt{\frac{k-1}{n-k+1}}}}{n} \tag{10}$$

So, to find k we have to calculate:

$$\begin{gathered} E\left(\frac{e^{X_{k:n}}}{\sum_{i=1}^{n} e^{X_{i:n}}}\right) \leq \in \\ \frac{e^{\sqrt{\frac{k-1}{n-k+1}}}}{n} \leq \in n\in \geq 1 \\ \sqrt{\frac{k-1}{n-k+1}} \leq ln(n\in) \\ k \leq \frac{1+(n+1)\ln^2(n\in)}{1+\ln^2(n\in)} \end{gathered} \tag{11}$$

The solution is an intuitive objective function based on the nodes' square distance that determines the optimal privacy recommendations. To do this, it is necessary to minimize the sum of the square errors in all pairs of bonds connecting the pairs of vertices:

$$\min_{U\in\mathbb{R}^{m\times d},V\in\mathbb{R}^{n\times d}} \sum_{(i,j)\in\text{obs}} \left(A_{ij} - \langle U_i, V_j\rangle\right)^2 \tag{12}$$

In this objective function, only the observed pairs (*i, j*) are added, i.e., the non-zero values in the feedback table. However, just summing up the prices is not a good idea. The aggregate table will have a minimal loss and produce a model that cannot make practical recommendations as it will generalize little.

To avoid the above weakness, we recommend the use of Weighted Matrix Factorization (WMF) to decompose the target in the following structure of the two sums (Abdi, Okeyo, and Mwangi 2018; Alexandridis, Siolas, and Stafylopatis 2017; Saadatniaki, Xin, and Khan 2020):

$$\min_{U\in\mathbb{R}^{m\times d},V\in\mathbb{R}^{n\times d}} \sum_{(i,j)\in\text{obs}} \left(A_{ij} - \langle U_i, V_j\rangle\right)^2 + w_0 \sum_{(i,j)\notin\text{obs}} \left(\langle U_i, V_j\rangle\right)^2 \tag{13}$$

It should be emphasized that w_0 is the overbalancing parameter of the two terms so that the target is not dominated by one or the other term.

The above general formulation is corrected by weighting specialized training examples, considering the frequency of optimal recommendations, to replace the objective function with the following:

$$\sum_{(i,j)\in\text{obs}} w_{i,j}\left(A_{i,j} - \langle U_i, V_j\rangle\right)^2 + w_0 \sum_{i,j\notin\text{obs}} \langle U_i, V_j\rangle^2 \tag{14}$$

Where $w_{i,j}$ is a function of the frequency of query i and item j.

Zero-Knowledge Proofs

Zero-Knowledge Proofs (Almuhammadi and Neuman 2005; Cao and Wan 2020; Schukat and Flood 2014; Tsai et al. 2019) have been presented as an alternative to interactive proof systems. Computation is carried out by exchanging messages between the entities Prover (P) and Verifier (V). Typically, P wishes to persuade V that a string is correct. If the latter only knows the first user's public key, there is no communication of private information (such as personal codes). P and V are probabilistic terms. Turing machines have infinite computing capability, while V is constrained to polynomial-complexity probabilistic computations (Qi and Chen 2009; Ryu, Kang, and Won 2021; Wan, Zhou, and Ren 2022).

This work uses the Zero Knowledge Proof format of the Schnorr digital public key signature (Li, Wu, and Yu 2021), which is based on the discrete logarithm problem and stands out for its simplicity and power. Schnorr Digital Signature Scheme (Jianhong et al. 2009; Kan and Shen 2003; Li, Wu, and Yu 2021) is a practical algorithm for creating signatures suitable for transactions

through terminals. It optimizes both signature creation and verification speed and digital signature bit size (Lin and Sako 2019).

The protocol assumes that both P and V know a generator g of a group of order q. P has a witness x so that $h = g^x$ and wants to prove it without revealing x. The process proceeds step by step as follows (Harikrishnan and Lakshmy 2019; He and Ge 2008):

(1) Commit $(\mathcal{P} \rightarrow \mathcal{V})$: Random selection $t \in \mathbb{R}_R \mathbb{Z}_q$ and calculation $y = g^t$. y is sent to $\mathcal{V}$.
(2) Challenge $(\mathcal{V} \rightarrow \mathcal{P})$: V randomly selects $c \in R\mathbb{Z}_q$ and sends it to.
(3) Response $(\mathcal{P} \rightarrow \mathcal{V})$: $\mathcal{P}$ calculates $s = t + cx(modq)$ and sends it to $\mathcal{V}$.
(4) $\mathcal{V}$ accepts if $g^s = yh^c$.

A schematic illustration of the Schnorr Protocol process is shown in Figure 1 below.

Completeness of the protocol can be demonstrated by simple replacement. Specifically, if $g^s = g^{t+cx} = g^t g^{cx} = yh^c$ are values known to $\mathcal{V}$. For the correctness of the protocol, we observe that an S who does not know x can execute it successfully with a probability of 1/q, which is negligible, as follows (Karthikeyan and Saraswady 2014; Ma 2020; Qi 2009; Ryu, Kang, and Won 2021):

(1) Initially chooses $c' \in_R \mathbb{Z}_q$
(2) Then selects $t \in R\mathbb{Z}_q$ and bind to $y = g^t h^{-c'}$
(3) If $\mathcal{V}$ chooses $c = c'$ then $\mathcal{P}$ sets $s = t$. We observe that it will accept since $yh^{c'} = g^t h^{-c'} h^{c'} = g^t = g^s$, but this can happen with a probability of exactly $1/q$.

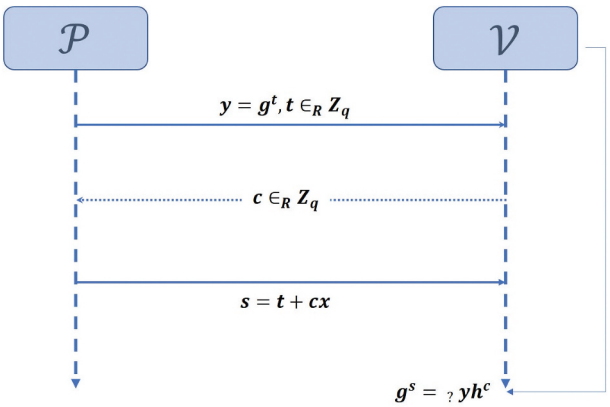

Figure 1. Schnorr Protocol.

Since they contain personal data and information, the study and analysis of signature patterns also require studying their security. The Schnorr protocol algorithm is an efficient cryptographic scheme applicable to all groups where the discrete logarithm problem is difficult to solve. Precisely an example of such an algorithm, while it stands out for its simplicity, is considered entirely secure even if the algorithm is public, since using a random permutation of the numbers $1, \ldots, k$, the algorithm is executed and chooses randomly, so that after some rounds run the new pairs to be nearly independent of the currency pairs. In particular, the digital signatures produced by the scheme resemble random numbers. The values x and$k$ are random numbers, and the value $h(r, m)$ is a random number as the output value of a condensation function, so the result is also a random number. That is, the value $s$is almost as if it is any number regardless of the message being entered and who the user is signing it with. Thus, Schnorr's signature protocol, using random variable values, which are uniformly distributed over an interval, undisclosed and non-repeated, enables strong security of systems where zero knowledge is required.

A significant advantage of the scheme is that the preprocessing algorithm, an essential factor in generating the signature, is independent of the message to be signed and can be performed at idle computer time. The preprocessing consists of raising to a power of a random number modulo a large number gives a remainder that speeds up the creation of the signature and require only the multiplication of a 72-bit integer by a 140-bit integer.

One of the notable advantages of the proposed scheme is the utilization of a preprocessing algorithm that plays a crucial role in generating the signature. What sets this algorithm apart is its independence from the message that needs to be signed, allowing it to be executed separately during idle computer time.

The preprocessing algorithm involves a series of operations, one of which is raising a random number to a power modulo a large number, resulting in a remainder. This operation has been specifically designed to expedite the signature creation process while maintaining the required security measures.

By raising a number to a power modulo a large number, the algorithm achieves several benefits:

(1) Computational Efficiency: The use of modular exponentiation, i.e., raising a number to a power modulo a large number, significantly speeds up the creation of the signature. This operation involves only the multiplication of a 72-bit integer by a 140-bit integer, reducing the computational complexity compared to alternative methods. As a result, the preprocessing algorithm can be efficiently executed even during idle computer time, making the most of available resources.
(2) Signature Generation Optimization: The remainder obtained from the modular exponentiation serves as a critical factor in generating the signature. By precomputing this remainder during the preprocessing

phase, the subsequent signature generation process can be streamlined. This optimization ensures that the signature creation does not impose excessive computational overhead when signing individual messages, contributing to the overall efficiency of the scheme.

(3) Security Considerations: Despite the computational efficiency gained through modular exponentiation, the security of the scheme remains robust. The large number and the random exponent utilized in the operation contribute to the strength of the signature generation process, safeguarding against potential attacks. The scheme ensures that the signature produced is both efficient and resistant to cryptographic vulnerabilities.

By incorporating the preprocessing algorithm, which is independent of the message being signed and employs modular exponentiation, the proposed scheme offers significant advantages in terms of computational efficiency and signature generation optimization. These optimizations reduce the computational burden and allow the system to utilize idle computer time effectively. Moreover, the scheme ensures the security and integrity of the generated signatures by employing a large number and random exponent in the modular exponentiation operation.

Schnorr signatures are proven secure and robust against chosen message attacks in the random oracle model. This implies that as long as the condensation function ideally behaves, the only way to "break" the Schnorr scheme is to solve the discrete logarithm problem.

Specifically, Schnorr signatures have been extensively studied and have been proven to offer both security and robustness against chosen message attacks in the random oracle model. This means that under this model, as long as the condensation function ideally behaves, the only known method to undermine the security of the Schnorr scheme is by solving the discrete logarithm problem.

The security of Schnorr signatures is of paramount importance in cryptography due to their widespread applications in various protocols and systems. The rigorous analysis and formal proof of security have demonstrated that Schnorr signatures provide a strong level of protection against adversarial attacks.

The random oracle model, a common framework for analyzing cryptographic schemes, assumes the existence of an idealized random oracle that produces unpredictable and unique outputs for each input. This model allows for a more tractable analysis of the security properties of cryptographic constructions.

By proving the security of Schnorr signatures against chosen message attacks in the random oracle model, researchers have shown that even if an adversary has the power to choose the messages for which they can

obtain signatures, they still cannot forge valid signatures or gain any advantage in breaking the scheme beyond solving the discrete logarithm problem.

The condensation function, a crucial component in Schnorr signatures, is responsible for compressing the message and reducing its size while preserving its uniqueness. As long as this function behaves ideally, meaning it produces consistent and deterministic outputs for each message, the security guarantees of the Schnorr scheme hold strong.

However, it's important to note that the security of Schnorr signatures is contingent upon the assumption that the discrete logarithm problem is computationally difficult. This assumption forms the basis of their security proof. The discrete logarithm problem is known to be a challenging mathematical problem, and the security of many cryptographic systems relies on the infeasibility of solving it efficiently.

In summary, Schnorr signatures have been rigorously proven to be secure and robust against chosen message attacks in the random oracle model. The cryptographic community has extensively analyzed their security properties, and their resilience to attacks is contingent upon the difficulty of the discrete logarithm problem. The strength of Schnorr signatures makes them a widely adopted and trusted cryptographic primitive in various domains.

Experiment: Schnorr Identification System

Following is an example to illustrate how the preprocessing algorithm, which is independent of the message being signed, can be implemented during periods of computer inactivity:

Let's consider a scenario where an educational institution wants to ensure the privacy of students' personal data while digitally signing their academic records. The preprocessing algorithm in this case would involve generating a unique signature pattern for each student based on their personal information.

1. Data Preprocessing: During periods of computer inactivity, the system can utilize idle computational resources to preprocess the students' data and generate their signature patterns. This process involves the following steps:

(a) Collecting Personal Data: The system collects personal data such as the student's name, address, contact details, disciplinary history, grades, and progress checks.
(b) Preprocessing Algorithm: The preprocessing algorithm processes the collected personal data to create a unique signature pattern for each student. This algorithm is designed to be independent of the message being signed, meaning it can generate the signature pattern without requiring the actual academic records or specific messages.

(c) Signature Pattern Generation: The preprocessing algorithm applies cryptographic techniques and mathematical transformations to the personal data, creating a distinctive signature pattern for each student. This pattern serves as a digital representation of their personal information, ensuring that the signature is unique to each individual.

2. Digital Signing Process: When it comes to digitally signing academic records or specific messages, the generated signature pattern can be combined with the appropriate cryptographic algorithms to create a secure and verifiable digital signature. The preprocessing algorithm, which was completed during periods of computer inactivity, is not involved in this signing process.

Let p, q prime numbers such that $q|p-1$. Also, g is a generator of the group Z_q^*.

(1) Private key: s such that $v = g - s(modp)$.
(2) Public key: $(p, q, g; v)$.

First, we give the following simplification (Almuhammadi and Neuman 2005; Schukat and Flood 2014; Tsai et al. 2019; Ulusoy et al. 2015):

1st step. Alice picks a random number $r \in \{1, 2, \ldots, q-1\}$ and sends it to Bob $x = g^r(modp)$.
2nd step. Bob chooses a random number $e \in \{1, 2\}$ and sends it to Alice.
3rd step. Alice calculates the number $y = r + es(modq)$ and sends it to Bob.
4th step. Bob performs the verification by checking the condition $g^y v^e(modp) = x$by doing the operations Z_q^* and specifically $g^y v^e = g^{r+es} g^{-se} = g^{r+es-es} = g^r = x$.

We assume that an educational system of three-motion identification is semantically safe (sound), if and only if Eve, knowing only the public key, can pass the authentication test with negligible probability (Kapassa and Themistocleous 2022). We will show that the security of the previous system depends only on the choice of e.

We suppose Eve predicts the correct $e' \in \{1, 2\}$. Then she can falsify Alice's identity. Eve chooses a random r from the set $\{1, 2, \ldots, q-1\}$ and guesses the correct e of Bob. She sets $y = r$ and calculates $g^y v^{e'}(modp)$ and sets it equal to x. Then the pair (x, y) passes the Bob test. Indeed, Bob will calculate $g^y v^{e'}$ which equals x. So, Eve is successful in the previous attack with a 1/2 chance. The protocol is not secure because Eve, with a not insignificant probability (1/2), succeeds in passing the authentication process (Hu et al. 2022).

We suggest the following reasonable modification (Schnorr) (Kan and Shen 2003; Ma 2020; Zhang et al. 2011).

According to the previous analysis, Eva can falsify Alice's identity with a probability of 2^{-t}. If we assume that t is 80, then Eva's previous attack has a negligible chance of success. This does not mean that the system is secure (Borisov et al. 2010). To prove that the system is sound, we must prove that Eva's chance of success cannot be increased by more than 2^{-t}.

1st step. Alice picks a random number $r \in \{1, 2, \ldots, q-1\}$ and sends it to Bob $x = g^r(modp)$.
2nd step. Bob chooses a random number $e \in \{1, 2, \ldots, 2^t\}$ and sends it to Alice.
3rd step. Alice calculates the number $y = r + es(modq)$ and sends it to Bob.
4th step. Bob does the verification by checking $g^y v^e(modp) = x$ by performing the operations on Z_q^* and specifically of $g^y v^e = g^{r+es} g^{-se} = g^{r+es-es} = g^r = x$.

The proof that with the proposed application, the system is sound, we will assume that there is a probabilistic algorithm A such that with input (pk, e), where e is random from the set $\{1, \ldots, 2^t\}$, returns with probability $\varepsilon > 2^{-t+1}$ a pair (x, y) that passes the authentication test is done in time $|A|$. Then, with a positive constant probability and in time $O(|A|/\varepsilon)$, the discrete logarithm $\log_g(v)$ in Z_q^*, can be calculated (Almuhammadi and Neuman 2005; Qi 2009; Schukat and Flood 2014).

According to the above view, the system is safe (for $t \geq 80$), because Eve cannot achieve anything better than randomly choosing e from the set $\{1, \ldots, 2^t\}$, unless she can calculate the discrete logarithm of v. In other words, if Bob behaves honestly (that is, he chooses e randomly) (Borsotti and Bjørn 2022). The system is sound (provided that calculating the discrete logarithm is difficult). We stabilize the public key pk. Algorithm A, other than pk, depends on an internal state of IS_A, which is a random binary word. Also, during the production of y the algorithm A depends on e. We define $S_A(IS_A, pk, e)$ a Boole function, which takes the value 1, when algorithm A succeeds for the input (pk, A, e); otherwise it is equal to 0. That is, $S_A(IS_A, pk, e) = 1$, when for the pair (IS_A, e) the algorithm A extracts a pair (x, y) such that it passes the authentication test of the identification scheme (Cao and Wan 2020; Chang 2021; Gao et al. 2021; Harikrishnan and Lakshmy 2019; Schukat and Flood 2014).

By decoupling the preprocessing algorithm from the actual signing process, the system gains several benefits:

(1) Time Efficiency: Since the preprocessing algorithm can be executed during idle periods, it maximizes the utilization of computational resources and optimizes system efficiency. It ensures that the signing process does not introduce additional delays or bottlenecks.
(2) Independence from Message Content: The preprocessing algorithm remains consistent regardless of the specific message being signed. This independence guarantees that the signature pattern is solely based on the student's personal data, making it reusable for different signing purposes.
(3) Enhanced Security: Separating the preprocessing algorithm from the signing process adds an additional layer of security. The signature pattern, which is created independently, contains no direct information about the message being signed, minimizing the risk of unauthorized access or information leakage.

Overall, by incorporating a preprocessing algorithm that is independent of the message being signed and utilizing computer inactivity periods, the system can efficiently generate signature patterns for students' personal data while ensuring privacy and security in the digital signing process.

On the other hand, the method does not provide 100% assurance that the claim is valid; it can reduce the likelihood of the Prover lying to practically zero, but not exactly zero. And the method utilized is so expensive that they need several contacts between the Prover and the Verifier, as well as a large number of calculations. As a result, it may be hard to run on sluggish or mobile devices. Finally, because the method is so effective at concealing secrets, they may lose access to them together. Assume that people "X," "Y," and "Z" know something like "Top-Secret." This assumption holds just among the three of them. Therefore, everyone knows only that these individuals know the Top-Secret, but no one knows "what it is "Top-Secret?" If three of them die, they may lose access to the "Top-Secret."

Some important considerations regarding the limitations and potential drawbacks of the proposed zero-knowledge proof intelligent recommendation system:

(1) Probability of Prover lying: While zero-knowledge proof techniques significantly reduce the likelihood of the Prover lying to practically zero, it is important to note that absolute certainty (100% assurance) is not achievable. Zero-knowledge proofs are designed to provide a high level of confidence in the validity of a claim without revealing sensitive information. However, there is always a small possibility of deception or errors in the cryptographic protocols used.
(2) Computational complexity: It is true that zero-knowledge proof protocols can involve multiple interactions between the Prover and the

Verifier, as well as a considerable number of calculations. This computational complexity can be resource-intensive and may pose challenges when running the system on slower or mobile devices with limited processing power. Efficient implementation and optimization techniques should be considered to mitigate these concerns.

(3) Risk of losing access to secrets: Zero-knowledge proof techniques excel at concealing secrets, but this advantage can also introduce the risk of losing access to the secrets altogether. In scenarios where multiple individuals collectively hold knowledge of a "Top-Secret," if some of them are no longer available (e.g., due to death), it can indeed result in the loss of access to that secret information. This highlights the importance of proper key management, contingency plans, and ensuring that critical information is appropriately shared among trusted parties.

It is crucial for any system, including the proposed zero-knowledge proof intelligent recommendation system, to consider these limitations and address them to the best extent possible. Further research and development efforts can focus on optimizing the computational efficiency of zero-knowledge proof protocols, enhancing key management strategies, and implementing backup mechanisms to mitigate the risks associated with losing access to essential secrets.

Overall, while zero-knowledge proof techniques offer valuable privacy preservation properties, their deployment should be accompanied by a comprehensive understanding of their limitations and appropriate measures to mitigate associated risks.

Conclusion

To eliminate the causes of leakage of sensitive personal data during e-learning systems, this research paper proposes a zero-knowledge proof intelligent recommendation system to protect students' data privacy in the digital age. The proposed approach incorporates an IRS, which uses an optimized form of the Matrix Factorization technique, calculated as an Eulerian Walk chart. Accordingly, the Schnorr Zero-Knowledge Proof format of the Schnorr digital key signature based on the discrete logarithm problem ensures personal data privacy when exchanging messages between educational entities.

Given the difficulties of implementing a comprehensive solution for preserving personal rights and sensitive personal information, this research effort proposes an advanced zero-knowledge proof intelligent recommendation system to secure students' data privacy in the digital era. The proposed method uses a heuristic methodology to create an algorithmic information filtering system, which seeks to predict the "score" or "preference" that a security expert would give to an element or action of the

educational environment based on these elements. It should be noted that this approach deals very precisely with the noisy dispersed points of inaccurate predictions/recommendations given after evaluating the behavioral features those other methods cannot manage. The implementation is based for the first time in the literature on the optimal utilization and combination of two highly efficient and fast computing systems, resulting in an integrated intelligent system of high reliability, while with the integration of Schnorr Zero-Knowledge Proof, encryption with the shape of the digital Schnorr's public key signature based on the discrete logarithm problem and stands out for its simplicity and power.

In contrast to existing recommendation algorithms, which conduct convolutions on feature matrices and the whole graph, the suggested method selects close nodes of a graph. It works more efficiently with local convolutions by dynamically constructing computational graphs. Convolutions on a node's whole neighborhood will generate a substantial computational graph. Traditional methods update a node's representation by aggregating information from its k-hop vicinity to decrease resource needs. The suggested technique mimics a random walk to choose frequently viewed material as the crucial region and then builds a convolutional network. Because k-hop areas often overlap, local convolution on nodes leads to repetitive computation. To prevent this, the proposed method maps all nodes without repeating calculations, links them to the respective upper-level nodes, and gets the embeddings of the upper-level nodes in each aggregation step.

The ideas for further study center primarily on the analysis and expansion of the model with intrinsic capabilities of employing quality characteristics that may highlight, without training, the methods of applying privacy regulations. Accordingly, for the automated system to take full advantage of the possibilities of the broader dependencies of the modeling of learning systems, multiple hyperparametric coordination techniques should also be explored for greater accuracy and efficiency. On the other hand, the remaining significant challenge is to make the zero-knowledge proofs efficient enough so that they do not create an unacceptable lag. Implementing specific new strategies for producing zero-knowledge proofs is critical, enabling the proofs to be exceedingly compact. A sophisticated assertion in linked spatiotemporal data, for example, takes up terabytes of space yet must be proved valid with just a few hundred bytes. Additionally, research and thorough experiments on the resistance of protocols in quantum attacks are required. Finally, eliminating the public key directory and subsequent "keyless" identification technique is the most challenging long-term prospect for future research.

Disclosure Statement

No potential conflict of interest was reported by the author.

Funding

The study was supported by the Research and Practice Project of Higher Education Teaching Reform in Henan Province in 2021 (No. 2021SJGLX901), i.e. Research and Practice on the Construction of Career Development Mechanism for Young Teachers in Personnel Agency of Higher Vocational Schools.

References

Abdi, M. H., G. Okeyo, and R. W. Mwangi. 2018. Matrix factorization techniques for context-aware collaborative filtering recommender systems: A survey. *Computer and Information Science* 11 (2):1. doi:10.5539/cis.v11n2p1.

Ahmad, T. 2020. Corona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity. *SSRN Electronic Journal Available at SSRN 3568830*. doi:10.2139/ssrn.3568830.

Alexandridis, G., G. Siolas, and A. Stafylopatis. 2017. Enhancing social collaborative filtering through the application of non-negative matrix factorization and exponential random graph models. *Data Mining and Knowledge Discovery* 31 (4):1031–59. doi:10.1007/s10618-017-0504-3.

Almuhammadi, S., and C. Neuman. 2005. Security and privacy using one-round zero-knowledge proofs. Seventh IEEE International Conference on E-Commerce Technology (CEC'05), Munich, Germany, 435–438. doi:10.1109/ICECT.2005.78.

Andergassen, M., G. Ernst, V. Guerra, F. Mödritscher, M. Moser, G. Neumann, and T. Renner. 2015. The evolution of e-learning platforms from content to activity based learning: The case of Learn@ Wu. 2015 International Conference on Interactive Collaborative Learning (ICL), Firenze, Italy, 779–784. doi:10.1109/ICL.2015.7318127.

Borisov, N., M. Klonowski, M. Kutyłowski, and A. Lauks-Dutka 2010. Attacking and repairing the improved modonions protocol. Paper presented at the Information, Security and Cryptology–ICISC 2009: 12th International Conference, Seoul, Korea, December 2-4, 2009, Revised Selected Papers 12.

Borsotti, V., and P. Bjørn. 2022. Humor and stereotypes in computing: An equity-focused approach to institutional accountability. *Computer Supported Cooperative Work (CSCW)* 31 (4):771–803. doi:10.1007/s10606-022-09440-9.

Cao, L., and Z. Wan. 2020. Anonymous scheme for blockchain atomic swap based on zero-knowledge proof. 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), Dalian, China, 371–374. doi:10.1109/ICAICA50127.2020.9181875.

Cao, X., H. Zhang, J. Shi, and G. Cui. 2008. Cluster heads election analysis for multi-hop wireless sensor networks based on weighted graph and particle swarm optimization. 2008 Fourth International Conference on Natural Computation, Jinan, China, 599–603. doi:10.1109/ICNC.2008.693.

Chang, B. 2021. Student privacy issues in online learning environments. *Distance Education* 42 (1):55–69. doi:10.1080/01587919.2020.1869527.

Chigada, J., and R. Madzinga. 2021. Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management* 23 (1):1–11. doi:10.4102/sajim.v23i1.1277.

Daras, G., A. Odena, H. Zhang, and A. G. Dimakis. 2020. Your local GAN: Designing two dimensional local attention mechanisms for generative models. 2020 IEEE/CVF

Conference on Computer Vision and Pattern Recognition (CVPR), Seattle, WA, USA, 14519–14527. doi:10.1109/CVPR42600.2020.01454.

Gabay, D., K. Akkaya, and M. Cebe. 2020. Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs. *IEEE Transactions on Vehicular Technology* 69 (6):5760–72. doi:10.1109/TVT.2020.2977361.

Gao, H., Z. Ma, S. Luo, Y. Xu, Z. Wu, and Z. Duan. 2021. BSSPD: A blockchain-based security sharing scheme for personal data with fine-grained access control. *Wireless Communications and Mobile Computing* 2021:1–20. doi:10.1155/2021/6658920.

Gong, X.-R., R.-C. Zhao, and L.-S. Lu. 2007. Communication optimization algorithms based on extend data flow graph. Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007), Qingdao, China, 3–8. doi:10.1109/SNPD.2007.168.

Harikrishnan, M., and K. Lakshmy. 2019. Secure digital service payments using zero knowledge proof in distributed network. 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 307–312. doi:10.1109/ICACCS.2019.8728462.

Hassanpour, A., M. Moradikia, H. Adeli, S. R. Khayami, and P. Shamsinejadbabaki. 2019. A novel end-to-end deep learning scheme for classifying multi-class motor imagery electro-encephalography signals. *Expert Systems* 36 (6):e12494. doi:10.1111/exsy.12494.

Hatzivasilis, G., S. Ioannidis, M. Smyrlis, G. Spanoudakis, F. Frati, L. Goeke, and T. Hildebrandt, G. Tsakirakis, F. Oikonomou, G. Leftheriotis. 2020. Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. *Applied Sciences* 10 (16):5702. doi:10.3390/app10165702.

He, Z., and L. Ge. 2008. ID-Based signature under the schnorr signature. 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing, Dalian, China, 1–3. doi:10.1109/WiCom.2008.1118.

He, Y., Y. Ye, P. Hanhart, and X. Xiu. 2017. Motion compensated prediction with geometry padding for 360 video coding. 2017 IEEE Visual Communications and Image Processing (VCIP), St. Petersburg, FL, USA, 1–4. doi:10.1109/VCIP.2017.8305088.

Hu, J., P. Zhu, Y. Qi, Q. Zhu, and X. Li. 2022. A patent registration and trading system based on blockchain. *Expert Systems with Applications* 201:117094. doi:10.1016/j.eswa.2022.117094.

Jianhong, Z., C. Hua, G. Shengnan, and G. Qin 2009. On the linkability of two schnorr type ID-Based blind signature schemes. Paper presented at the 2009 International Forum on Computer Science-Technology and Applications.

Kan, H., and H. Shen. 2003. On Schnorr-Adleman lattice. Paper presented at the Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Chengdu, China, Applications and Technologies. doi:10.1109/PDCAT.2003.1236246.

Kapassa, E., and M. Themistocleous. 2022. Blockchain technology applied in IoV demand response management: A systematic literature review. *Future Internet* 14 (5):136. doi:10.3390/fi14050136.

Karthikeyan, M., and D. Saraswady. 2014. Sphere decoding using threshold based Schnorr-Euchner enumeration in MIMO system. 2014 International Conference on Recent Trends in Information Technology, Chennai, India, 1–4. doi:10.1109/ICRTIT.2014.6996088.

Lam, T. Y., J. Clampitt, Y.-C. Cai, and B. Li. 2015. Voids in modified gravity reloaded: Eulerian void assignment. *Monthly Notices of the Royal Astronomical Society* 450 (3):3319–30. doi:10.1093/mnras/stv797.

Li, W., H. Guo, M. Nejad, and C.-C. Shen. 2020. Privacy-preserving traffic management: A blockchain and zero-knowledge proof inspired approach. *IEEE Access* 8:181733–43. doi:10.1109/ACCESS.2020.3028189.

Li, D., H. Guo, Z. Wang, and Z. Zheng. 2021. Unsupervised fake news detection based on autoencoder. *IEEE Access* 9:29356–65. doi:10.1109/ACCESS.2021.3058809.

Lin, J., H. Pu, Y. Li, and J. Lian. 2018. Intelligent recommendation system for course selection in smart education. *Procedia Computer Science* 129:449–53. doi:10.1016/j.procs.2018.03.023.

Lin, D., and K. Sako.2019.Public-Key Cryptography–PKC 2019,*22nd IACR international conference on practice and theory of public-key cryptography.Beijing, China*:April 14-17 *2019*, *Proceedings, Part* II (Vol. 11443) Springer.10.1007/978-3-030-17259-6.

Li, C., Y. Wu, and F. Yu. 2021. An improved Schnorr-based multi-signature scheme with application to blockchain. 2021 IEEE 3rd International Conference on Civil Aviation Safety and Information Technology (ICCASIT), Changsha, China, 858–863. doi:10.1109/ICCASIT53235.2021.9633663.

Li, W., L. Xia, and Y. Huang. 2020. An Adaptive ant colony optimization in knowledge graphs. 2020 IEEE International Conference on Knowledge Graph (ICKG), Nanjing, China, 26–32. doi:10.1109/ICBK50248.2020.00014.

Ma, T. 2020. White-box Schnorr signature for internet of things security. 2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), Harbin, China, 1939–1942. doi:10.1109/ICMCCE51767.2020.00425.

Menci, N. 2002. An Eulerian perturbation approach to large-scale structures: Extending the adhesion approximation. *Monthly Notices of the Royal Astronomical Society* 330 (4):907–19. doi:10.1046/j.1365-8711.2002.05133.x.

Murphy, K. P. 2012. *Machine learning: A probabilistic perspective*, vol. 25. Cambridge, MA, USA: MIT press.

Pasquet, M., F. Maia, E. Riviere, and V. Schiavoni 2014. Autonomous multi-dimensional slicing for large-scale distributed systems. Paper presented at the Distributed Applications and Interoperable Systems: 14th IFIP WG 6.1 International Conference, DAIS 2014, Held as Part of the 9th International Federated Conference on Distributed Computing Techniques, DisCoTec 2014, Berlin, Germany, June 3-5, 2014, Proceedings 14.

Perez, M., S. Avila, D. Moreira, D. Moraes, V. Testoni, E. Valle, and S. Goldenstein, A. Rocha. 2017. Video pornography detection through deep learning techniques and motion information. *Neurocomputing* 230:279–93. doi:10.1016/j.neucom.2016.12.017.

Pop, C., T. Cioara, M. Antal, and I. Anghel. 2020. Trading Energy as a Digital Asset: A Blockchain based Energy Market. *Cryptocurrencies Blockchain Technol. Appl. Decentralization Smart Contract* 261–79.

Qi, C. (2009). A zero-knowledge proof of digital signature scheme based on the elliptic curve cryptosystem. 2009 Third International Symposium on Intelligent Information Technology Application, Nanchang, China, 612–615. doi:10.1109/IITA.2009.505.

Qi, M., and B. Chen. 2009. Construction of safe patent trading platform based on zero-knowledge proof. 2009 Asia-Pacific Conference on Information Processing, Shenzhen, China, 627–630. doi:10.1109/APCIP.2009.288.

Rafiei, M. H., and H. Adeli. 2017. NEEWS: A novel earthquake early warning model using neural dynamic classification and neural dynamic optimization. *Soil Dynamics and Earthquake Engineering* 100:417–27. doi:10.1016/j.soildyn.2017.05.013.

Ryu, H., D. Kang, and D. Won. 2021. On a partially verifiable multi-party multi-argument zero-knowledge proof. 2021 15th International Conference on Ubiquitous Information Management and Communication (IMCOM), Seoul, Korea (South), 1–8. doi:10.1109/IMCOM51814.2021.9377407.

Saadatniaki, F., R. Xin, and U. A. Khan. 2020. Decentralized optimization over time-varying directed graphs with row and column-stochastic matrices. *IEEE Transactions on Automatic Control* 65 (11):4769–80. doi:10.1109/TAC.2020.2969721.

Schukat, M., and P. Flood. 2014. Zero-knowledge proofs in M2M communication, 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014), Limerick, 269–273. doi:10.1049/cp.2014.0697.

Sun, X., F. R. Yu, P. Zhang, Z. Sun, W. Xie, and X. Peng. 2021. A survey on zero-knowledge proof in blockchain. *IEEE Network* 35 (4):198–205. doi:10.1109/MNET.011.2000473.

Tahiri, J. S., S. Bennani, and M. K. Idrissi. 2016. An assessment system adapted to differentiated learning within massive open online courses using psychometric testing. 2016 15th International Conference on Information Technology Based Higher Education and Training (ITHET), Istanbul, Turkey, 1–7. doi:10.1109/ITHET.2016.7760741.

Tsai, Y. C., R. Tso, Z.-Y. Liu, and K. Chen. 2019. An improved non-interactive zero-knowledge range proof for decentralized applications. 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), Newark, CA, USA, 129–134. doi:10.1109/DAPPCON.2019.00025.

Ugurlu, B., and A. Kawamura. 2010. Eulerian ZMP resolution based bipedal walking: Discussions on the intrinsic angular momentum rate change about center of mass. 2010 IEEE International Conference on Robotics and Automation, Anchorage, AK, USA, 4218–4223. doi:10.1109/ROBOT.2010.5509427.

Ulusoy, Ö., A. U. Tansel, E. Arkun, Ö. Ulusoy, A. U. Tansel, and E. Arkun. 2015. *Recommendation and search in social networks*. Springer International Publishing. doi: 10.1007/978-3-319-14379-8.

Wang, Q., and K. Demertzis. 2022. Privacy leaks protection in music streaming services using an intelligent permissions management system. *Computational Intelligence and Neuroscience* 2022:1–7. doi:10.1155/2022/5027256.

Wang, J., Z. Tan, X. Li, and Y. Hu. 2020. Differential privacy preservation in interpretable feedforward-designed convolutional neural networks. 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 631–638. doi:10.1109/TrustCom50675.2020.00089.

Wan, Z., Y. Zhou, and K. Ren. 2022. Zk-AuthFeed: Protecting data feed to smart contracts with authenticated zero knowledge proof. *In IEEE Transactions on Dependable and Secure Computing* 20 (2): 1335–1347. doi:10.1109/TDSC.2022.3153084.

Wehrmann, J., G. S. Simões, R. C. Barros, and V. F. Cavalcante. 2018. Adult content detection in videos with convolutional and recurrent neural networks. *Neurocomputing* 272:432–38. doi:10.1016/j.neucom.2017.07.012.

Xue, Y., Q. Zhang, and F. Neri. 2021. Self-adaptive particle swarm optimization-based echo state network for time series prediction. *International Journal of Neural Systems* 31 (12):2150057. doi:10.1142/S012906572150057X.

Yamamoto, M., T. Uchitane, and T. Hatanaka. 2012. An experimental study for multi-objective optimization by particle swarm with graph based archive. 2012 Proceedings of SICE Annual Conference (SICE), Akita, Japan, 89–94.

Yan, K., H.-C. Wu, H. Xiao, and X. Zhang. 2016. Novel robust band-limited signal detection approach using graphs. *IEEE Communications Letters* 21 (1):20–23. doi:10.1109/LCOMM.2016.2618871.

Zhang, Y., and K. Demertzis. 2022. Increasing cyber defense in the music education sector using blockchain zero-knowledge proof identification. *Computational Intelligence and Neuroscience* 2022:1–7. doi:10.1155/2022/9922167.

Zhang, L., J. Li, L. Chen, and Y. Zhou. 2011. A undividable electronic cash scheme based on Schnorr digital signature. 2011 International Conference on Computer Science and Service System (CSSS), Nanjing, 2951–2954. doi:10.1109/CSSS.2011.5974728.

Zheng, X., X. Yin, and K. Demertzis. 2022. A privacy-preserved variational-autoencoder for DGA identification in the education industry and distance learning. *Computational Intelligence and Neuroscience* 2022:1–8. doi:10.1155/2022/7384803.

Zoolfakar, A., and F. Sulaiman. 2009. Providing differentiated learning experiences through e-Learning on solid state devices course. 2009 International Conference on Engineering Education (ICEED), Kuala Lumpur, Malaysia, 138–142. doi:10.1109/ICEED.2009.5490598.