ANALYSIS OF INFORMATION TECHNOLOGY IN DETERMINING THE EFFECTIVENESS OF TALENTED REQUIREMENTS

Yusupova Zamira
Tashkent University of Information Technology named after Mukhammad al-Khwarazmi,
yusupovaz677@gmail.com
+998909337461
Yusupov Baxtiyor
Tashkent State Technical University Named After Islam Karimov
tojiakbarova@gmail.com
+998933858491

Abstract. With the help of information technology, it is possible to quickly and accurately collect information about talented students. Information technology helps to identify the strengths and weaknesses of each student in the educational process. Through this, each student will be able to draw up an individual program, choose the most suitable methods for developing his talent. This article incorporates blockchain, cloud, machine learning, Artificial Intelligence and information technology. These technologies have been cited in detail in determining their talent requirements.

Keywords: Artificial Intelligence, machine learning, cloud, blockchain, analysis, efficiency, information, technology.

I. INTRODUCTION

Gifted students differ from others because of their extraordinary ability and potential. The place which the analysis occupies is very important because their effectiveness is necessary to be established and correctly estimated. The main reasons and benefits can be represented in the following aspect:

1. Collection and data analysis: information technology provides an avenue for amassing and analyzing vast amounts of data relating to the reading process and activities of requirements. It is for example possible to use electronic assessment systems to record and analyze reading results through which strengths and weaknesses of the requirements will be found.
2. Customized training: With the aid of IT, the training can be provided based on personalized needs and requirements. For example, on the websites and portals online, students have been given proper reading material. This makes it possible for talented students to choose the methods and speed that suit them.
3. Visualization of results: it is possible to visually show the success of requirements using IT tools. Graphs, diagrams and other indicators clearly show the changes and achievements of demand. This will help teachers and educational institutions monitor the progress of demand.
4. More interactive teaching opportunities: it is —possible to attract students through interactive textbooks, simulations, and games using information technology. This increases the motivation of the requirements and makes the reading process more interesting and effective.
5. Distance education: gifted students can be from different regions. Information technology contributes to the implementation of distance learning, which ensures that learning for students does not depend on time and place. Distance education: gifted students can be from different regions. Information technology helps in the implementation of distance learning, which ensures that learning for students does not depend on time and place.
6. Opinions and recommendations: with the help of artificial intelligence (AI) and machine learning technologies, it is possible to analyze student activities and make recommendations

for teachers and mentors. Through this, students identify their strengths and areas necessary for development.

In this way, information technology provides ample opportunities for the analysis and development of gifted students, increases efficiency and further perfects the educational system. In the use of Information Technology in determining the effectiveness of their talent requirements, a number of technologies are listed below.

*Blockchain i*s a technology that involves collecting data into a chain of sequential blocks with protection using cryptographic ciphers. At the same time, data loops are not stored on a separate server, but are available simultaneously on all devices connected to the network. Blockchain is an independent system that does not require the operation of third parties. In the process of creating a blockchain, the main goal of developers is to distance themselves from intermediaries [3].

Blockchain technology can be used:

1. carrying out financial transactions with money;
2. conclusion of contracts and agreements;
3. implementation of the process of various commercial operations;
4. purchase of goods and services;
5. to exchange confidential information;
6. to register an insurance policy;
7. protection of property rights, as well as their transfer to a new owner;
8. personal Data Management;
9. ensuring the security of intellectual property;
10. to help create archives of documents.
11. working with blockchain technology usage tables and putting them into practice [3].

Cloud computing virtualization technology provides efficient resources for end users. Cloud computing characteristics include manageability, scalability, and availability. In addition, cloud computing has advantages such as cost savings, on-demand service, convenience, versatility, multitenancy, flexibility, and stability. Cloud computing mainly provides three service delivery models and four development patterns: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), Public Cloud, private cloud, hybrid cloud, community cloud, and virtual private cloud.

IaaS handles computer hardware (network storage, virtual server /computer, data center, processor, and memory) as a service and enables infrastructure scalability and resource provisioning challenges without significant capital investment and time. IaaS also focuses on firewall, intrusion detection, virtual machine monitoring, and other areas of security [1].

PaaS resides in service model middleware and provides services in the form of development tools, frameworks, architectures, programs, and IDEs. PaaS faces many challenges such as relationships with third parties, lifecycle design, and security of the underlying infrastructure.

SaaS is a collection of remote computing services that enables third-party vendors to remotely deploy applications. The customer can use the Internet for cloud service provider applications in the cloud infrastructure.

Private Cloud: cloud computing is runs and managed within the data center of an organization, which is referred to as a private cloud. In a private cloud, customer and supplier relationships are easier to identify because the infrastructure is owned and operated by the same organization.

Public cloud: enterprises, academia or government organizations have a public cloud environment, which can cause many problems because users do not know the locations or owners of resources, which increases the difficulty of protecting resources from attacks.

Hybrid cloud: it is a combination of two or more clouds (public, private, community). A hybrid cloud provides the advantages of differentcloud deployment models. However, when accessing entities via the Internet, a hybrid cloud is better organized and more secure than a public cloud.

Virtual private cloud: it is a semi private cloud with fewer resources that is composed of a virtual private network (VPN). This cloud is the shared resource pool allocated in the cloud environment [2].

Artificial Intelligence (AI) is the field of computer science focused on creating machines and software capable of performing tasks that usually require human intelligence. This includes reasoning, learning, problem-solving, perception, and language understanding. Key Components of AI:

1. Machine Learning: It's the ability of AI machines to improve their performance automatically through the learning process from data experience without explicit programming.
2. Natural Language Processing: The ability of computers to understand, interpret, and generate human language is called NLP. It covers applications such as virtual assistants, machine translation, and sentiment analysis.
3. Computer Vision: The technology puts the sense into the AI to interpret visual information from the world, such as recognizing objects in images or videos using technology like Facial Recognition.
4. Robotics: AI applied to robotics makes the machines capable of operating themselves. This covers all levels: from industrial robots to self-driving cars.
5. Expert Systems: A knowledge-based system with an added knowledge base of a specific expert that acts like decisions by a human expert, such as diagnosing ailments or financial planning [5].

The integration of Blockchain, AI, and Cloud Technologies in IT will definitely upgrade different ways in which organizations work out the talent requirements and their effective appraisal. It helps streamline the process of recruitment, performance tracking, skills development, and workforce management. Here's how each of these technologies plays its role in determining the effectiveness of the talent requirements:

Artificial Intelligence Artificial intelligence comes at the forefront in the analytics of talent needs to help an organization in defining, predicting, and optimizing talent managing processes. This is how:

1. Talent Acquisition and Recruitment: AI-powered recruitment tools automatically screen resumes to filter in a candidate on the job description. It can even conduct the first level of interviews. Based on previous hiring decisions, AI may even get better at refinement in an iterative manner.
2. Predictive Analytics: AI will make predictions about who will perform well in the future based on patterns which emerge from candidates' past experiences, education, and skills, among others. This helps the organization to onboard and hire people who have more chances of succeeding.
3. Skills Gap Analysis: AI can analyze the current talent pool and identify gaps in skills or competencies required by the organization. This analysis helps HR departments forecast the types of roles they will need to fill and what skills those roles will demand.
4. Performance Tracking and Development: AI can monitor employee performance by analyzing productivity data, feedback, and even natural language in communications. AI-driven systems can suggest areas for training or development and help organizations retain top talent by offering personalized growth opportunities [6].

II. METHOD OF RESEARCH

Combined Use of Blockchain, AI, and Cloud in Talent Management:

1. These are technologies that can be incorporated to provide a more integrated, efficient, and effective approach to talent management. Here's how they interface:

2. AI-driven insights identify what skills are needed by the organization in the future, while tracking and verification take place on the blockchain, checking the validity and authenticity of the credentials.

3. Cloud platforms would work as the base over which data about talent management is based and shared. That data, in turn, would be analyzed by AI, while blockchain will be responsible for making recordings of qualifications and contracts secure and transparent.

4. Blockchain smart contracts can independently take action based on payroll, hiring, and training programs based on AI insights, while all data generated will be stored and shared in the cloud.

Effectiveness of talent requirements:

1. These technologies increase the effectiveness of the determination of talent requirements in a number of ways: Improved Accuracy: While AI can analyze volumes of data to predict which skills and roles will be required for future projects, blockchain delivers accuracy and authenticity of employee data.

2. Efficiency: Cloud technologies provide the infrastructure on which AI and blockchain integration goes through with ease; hence, it makes talent management smooth, right from hiring to talent development.

3. Security and Trust: Blockchain ensures that talent information is secure, open, and tamper-proof; hence, trust in candidates and employers will be earned.

4. Data-driven decision: Artificial intelligence and cloud technologies allow the human resource department to introduce data-driven decisions on hiring, training, and performance management while eliminating biases and boosting effectiveness.

III. RESEARCH RESULTS

The following table analyzes different technologies based on various important aspects.

TABLE 1. General analysis of cloud computing, blockchain and artificial intelligence (AI):

Aspect	Cloud Computing	Blockchain	Artificial Intelligence (AI)
Definition	A network of remote servers to store, manage, and process data.	A decentralized, distributed ledger that records transactions across multiple computers.	Simulation of human intelligence in machines that can learn, reason, and make decisions.
Core Purpose	To provide on-demand access to computing resources and storage via the internet.	To enable secure, transparent, and tamper-proof transactions without a central authority.	To enable machines to perform tasks that typically require human intelligence, such as learning, decision-making, and automation.
Security	Centralized security protocols; vulnerability in data centers, but encryption and multi-factor authentication are common.	Highly secure due to its decentralized nature, cryptographic hashing, and immutability of data.	Security varies based on data privacy practices; AI models can be vulnerable to adversarial attacks, model theft, and data breaches.
Scalability	Highly scalable; resources can be increased or decreased according to demand, e.g., server capacity, storage.	Limited scalability; blockchain systems may experience slower processing speeds as they grow.	Scalable for large data sets and tasks, but AI models require extensive computational power for training, especially deep learning models.
Speed	Fast processing and retrieval of data, though may depend on internet speed and server load.	Slower due to the need to validate and record transactions on multiple nodes across the network.	Can be fast in execution, but training complex models (especially deep learning) can take time and computing power.
Flexibility	Highly flexible in terms of storage, computational resources, and service deployment (IaaS, PaaS, SaaS).	Limited flexibility; mainly used for decentralized transactions and recording data, but growing use cases (smart contracts, DeFi).	Highly flexible, capable of handling diverse tasks, including natural language processing, computer vision, and autonomous decision-making.
Cost	Pay-as-you-go pricing models; costs can vary based on resource usage, data storage, and network traffic.	Transaction fees for processing on the network; can vary by blockchain type (e.g., Ethereum vs. Bitcoin).	Development, training, and deployment costs can be high, particularly for complex AI models and large data sets.
Applications	Cloud storage, computing services, SaaS, IaaS, PaaS, remote collaboration, enterprise applications, and big data processing.	Cryptocurrency, supply chain tracking, decentralized finance (DeFi), digital identity, voting systems, and auditing.	Image recognition, natural language processing, predictive analytics, robotics, recommendation systems, autonomous systems.

Transparency	Limited transparency; controlled by service providers, with billing transparency, but limited on backend operations.	High transparency; transactions are publicly recorded and can be verified by all participants in the network.	Low transparency; AI models, especially deep learning, can be considered "black boxes," making it hard to understand decision-making processes.
Decentralization	Centralized, controlled by service providers (e.g., AWS, Google Cloud, Microsoft Azure).	Decentralized by design; no single authority controls the data, transactions, or network.	Mostly centralized (corporate-controlled AI models), but emerging decentralized models like federated learning are being explored.
Integration	Easy integration with other cloud services and on-premise solutions (APIs, third-party services, data lakes).	Integrates with decentralized applications (dApps), cryptocurrency wallets, and smart contracts.	Integrates with various systems for automation, decision-making, data analysis, customer service (chatbots), and more.
Reliability	High reliability with built-in redundancies, failover, and data backup across multiple data centers.	Reliable due to blockchain's immutable ledger and decentralized nature, reducing the risk of data tampering.	Reliability depends on the model, data quality, and training; errors may occur if data is biased or incomplete.
Governance	Managed and controlled by centralized service providers, subject to regulations and compliance standards (GDPR, HIPAA).	Governance is decentralized, usually through consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS), with no central authority.	Governance is centralized in most AI models; however, frameworks and policies are being developed to address issues like fairness, accountability, and transparency.
Data Storage	Cloud offers extensive data storage options (e.g., object storage, databases) with flexible scaling capabilities.	Blockchain stores data in blocks across multiple nodes, ensuring redundancy but is limited in storage capacity per block.	AI models rely on large datasets for training; data is stored in various formats, often requiring cloud infrastructure for scalability.
Future Potential	Highly promising with advancements in edge computing, hybrid cloud, and AI cloud services, driving innovation in various industries.	Blockchain's potential is growing in areas like supply chain transparency, digital assets, and secure transactions, with applications in finance, healthcare, and governance.	AI is set to revolutionize industries, enhancing decision-making, automating processes, and creating new human-computer interaction possibilities, especially in robotics, healthcare, and autonomous systems.

TABLE 2 General analysis of cloud computing, blockchain, and artificial intelligence in relation to information security

Aspect	Cloud Computing	Blockchain	Artificial Intelligence (AI)
Security Model	Centralized security controls; relies on service providers to implement security measures like encryption and multi-factor authentication.	Decentralized security model; uses cryptography and consensus mechanisms to ensure data integrity and security.	Dependent on security of data used for training, the algorithms themselves, and access control of AI systems.
Data Encryption	Strong encryption (in-transit and at-rest) is provided by cloud providers; however, encryption keys are managed by the provider unless specified otherwise.	Blockchain uses strong encryption and cryptographic hashing to secure transactions and ensure immutability.	Data used in AI (especially for training) can be encrypted, but the model itself may not always be encrypted, leaving vulnerabilities.
Access Control	Identity and access management (IAM) frameworks are common, allowing granular control over user access to resources.	Public/private key pairs are used to authenticate users and ensure secure transactions.	AI systems require robust access control to limit who can manipulate models, access sensitive data, or deploy systems.
Data Integrity	Cloud service providers implement data integrity measures, but data integrity is at risk if the provider is compromised.	Blockchain ensures data integrity by recording transactions on a decentralized ledger, making data tampering almost impossible.	AI systems depend on the quality and integrity of data for training. Poor data integrity can lead to inaccurate or biased model outputs.
Authentication	Multi-factor authentication (MFA) is commonly used for access to cloud services, along with role-based access controls (RBAC).	Blockchain uses cryptographic signatures (e.g., public/private keys) for authentication, making identity verification secure.	AI systems require proper authentication protocols to ensure that unauthorized users do not manipulate models or results.
Privacy	This could bring in issues of privacy since critical information might leak from these cloud servers. A lot of providers offer privacy; however, the dependency on a third-party manager remains.	Blockchain offers strong privacy features, particularly with pseudonymity or privacy coins; however, it can expose transaction history unless special privacy-focused protocols are used.	AI models often rely on large datasets, raising privacy concerns if personal or sensitive data is not properly anonymized or protected.
Compliance	Cloud providers often comply with regulatory standards (e.g., GDPR, HIPAA, SOC 2) to ensure data protection and privacy.	Blockchain's decentralized nature complicates compliance with traditional regulations, but new standards are emerging for decentralized systems.	AI faces challenges in compliance due to evolving regulations (e.g., GDPR's provisions on data processing, fairness, and transparency).
Attack Surface	Cloud computing has a broad attack surface due to its widespread infrastructure, including APIs, virtual machines, and storage services.	Blockchain's attack surface is smaller but still includes potential vulnerabilities in consensus mechanisms and smart contracts.	AI systems can be attacked by adversarial methods, which involve exploiting vulnerabilities in models or data, leading to incorrect outputs.
Redundancy and Backup	Cloud services often provide automated backup and disaster recovery options to ensure data availability and security.	Blockchain networks are highly redundant by design, as every node holds a copy of the ledger, ensuring data availability.	AI models require robust backup mechanisms to prevent model corruption or loss, particularly if a

			system is compromised or attacks are attempted.
Data Storage	Data is stored on remote servers and may be vulnerable if not properly encrypted or managed by trusted cloud providers.	Blockchain data is immutable and distributed across many nodes, making it resilient to attacks or single points of failure.	AI systems store large datasets used for training, which can be a target for theft or manipulation if not secured properly.
Resilience	Cloud computing services are often highly resilient, with built-in redundancy, failover, and disaster recovery systems.	Blockchain is resilient due to its decentralized nature, but it may struggle with scalability issues under heavy transaction loads.	AI systems' resilience depends on the robustness of models to adversarial attacks or data manipulation and the quality of the underlying training data.
Auditing and Monitoring	Cloud providers typically offer tools for monitoring and auditing user activities, access logs, and data transfers.	Blockchain's public ledger inherently allows for auditing and monitoring of all transactions on the network, providing full transparency.	AI systems require continuous monitoring to detect anomalies, adversarial attacks, and potential breaches in model integrity.
Incident Response	Cloud services offer incident response protocols, but the shared responsibility model means the provider and customer share this duty.	Blockchain, though allowing distributed control, may have no single entity to handle incident response. Events like a hard fork or protocol changes could be employed to mitigate an ongoing attack.	AI models need continuous monitoring and rapid responses to adversarial attacks, data poisoning, and manipulations.
Risk Management	Risk management is shared between the provider and the consumer, with the provider ensuring infrastructure security and the consumer ensuring application-level security.	Blockchain provides transparency, making risk management easier for transactions, but regulatory compliance and security threats can remain challenging.	AI risk management involves addressing model fairness, robustness against attacks, and the prevention of unintended consequences from misused algorithms.
Governance	Governance in cloud computing is generally centralized, controlled by the provider, with shared responsibility between the provider and consumer for security measures.	Blockchain's governance is decentralized and varies by blockchain type (e.g., Bitcoin, Ethereum), where consensus mechanisms control the network.	AI governance often remains centralized, typically managed by organizations or governments to regulate fairness, transparency, and ethical considerations in AI systems.

Cloud Computing has a very strong and centric security model, through powerful encryption, controls in access, and compliance features, but brings up concerns regarding its wide attack surface area and dependence on third-party providers.

It has provided decentralized security of data with cryptography, integrity, and transparency, but there also arise challenges on scalability issues, regulatory issues, or even privacy in specific use cases.

AI introduces new challenges in data privacy, integrity within the model, and adversarial threats. Model robustness and regulatory compliance in AI models are critical for secure AI deployment.

Those are strengths and weaknesses in the Information Security world that complement each other in use, like how AI models can be made more secure by Blockchain or upsaling AI on the cloud for much stronger encryption and versions.

TABLE 3. Application of cloud computing, blockchain, and AI in countries (2023-2024)

Country	Cloud Computing	Blockchain	Artificial Intelligence (AI)
United States	Leading in cloud services (AWS, Azure, Google Cloud)	Major hub for cryptocurrency (Bitcoin, Ethereum), DeFi	AI in healthcare, finance, autonomous vehicles, and smart cities
	Multi-cloud and hybrid cloud adoption	Growing NFT market, DeFi applications, and blockchain regulation	AI-driven automation in manufacturing, retail, and cybersecurity
China	Strong presence with Alibaba Cloud and Tencent Cloud	Digital Yuan (state-backed cryptocurrency)	AI in surveillance, smart cities, automated vehicles
	Increasing adoption of cloud computing in AI, IoT, and 5G	Blockchain for government applications and financial systems	Expansion in AI-powered automation and AI-driven national projects
European Union	Adoption of multi-cloud for data sovereignty and GDPR compliance	Active blockchain regulation (MiCA) and support for digital assets	AI in finance, healthcare, and manufacturing automation
	Cloud-native technology adoption, particularly in AI and IoT	Blockchain as a tool for identity management, e-voting, supply chain	Strong focus on AI ethics, regulations, and AI governance
India	Growth in cloud computing for e-commerce, healthcare, and education	Adoption of blockchain for supply chain, agriculture, finance	AI in healthcare, agriculture, and education
	Increasing use of cloud-based AI in startups and innovation	Digital India program exploring blockchain for government services	Government initiatives to drive AI adoption across industries
Japan	High adoption of cloud solutions in enterprise and IoT	Blockchain used in finance (cryptocurrency, digital yen)	AI in robotics, automated manufacturing, and autonomous vehicles

	Integration of cloud with AI for smart cities and healthcare	Focus on blockchain for governance and secure transactions	Government focus on AI in public services and smart cities
	Strong cloud infrastructure for AI/ML research	Decentralized Finance (DeFi) platforms emerging in Japan	AI-driven robotics and advanced technology solutions
South Korea	Leading cloud infrastructure with Kakao and Naver Cloud	Blockchain used in gaming, finance, and logistics	AI in robotics, cybersecurity, smart cities, and education
	Cloud-native apps and 5G network integration with AI	NFT platforms gaining popularity and blockchain-powered supply chains	Growing AI applications in autonomous systems and public services
United Kingdom	Major adoption of cloud solutions across healthcare, education, and finance	Blockchain in finance, e-commerce, and legal services	AI for fintech, healthcare, and autonomous transport
	Focus on multi-cloud and hybrid cloud adoption	Government regulatory push for blockchain (MiCA)	AI and big data analytics for financial markets
Australia	Expansion of cloud computing for data sovereignty and data centers	Blockchain adoption for supply chain, finance, and energy	AI in agriculture, mining, healthcare, and defense
	High demand for cloud infrastructure to support AI/ML projects	Blockchain's use for traceability in agriculture and financial services	AI-driven environmental solutions and energy management
Canada	Strong adoption of cloud computing across finance, healthcare, and education	Blockchain for supply chain transparency and financial services	AI in healthcare, clean tech, and fintech
	Cloud-native solutions driving AI-driven innovation in finance and energy	Use of blockchain for public health and government records	AI research on AI governance, predictive healthcare, and climate
Brazil	Growth in cloud computing for e-commerce, finance, and education	Adoption of blockchain for digital identity, cryptocurrency	AI in agriculture, finance, and education
	Emerging cloud services for AI and IoT integration	Blockchain projects focused on financial inclusion and government use	Focus on AI in agriculture and smart cities

TABLE 4. Application in education in Uzbekistan based on 2023-2024 cloud computing, general analysis of Blockchain and artificial intelligence (AI) technologies

Aspect	Cloud Computing	Blockchain	Artificial Intelligence (AI)
Key Applications	Cloud-based learning management systems (LMS) for schools and universities.	Blockchain for secure academic credentials and diploma verification	AI-powered personalized learning and tutoring systems
	Use of cloud storage for student records, and collaborative tools.	Blockchain for educational certificates to prevent fraud and ensure integrity	Adaptive learning platforms using AI to customize content for students
Government Initiatives	Uzbekistan's Digital Transformation strategy promotes cloud adoption in education.	Government exploring the use of blockchain for transparent education systems	National AI strategy includes AI development in education for future workforce development
	Cloud solutions for e-learning platforms and virtual classrooms.	Pilot projects to use blockchain for secure diploma issuance and student records	AI curriculum in schools and universities to prepare students for future jobs
Industry Adoption	Cloud-based e-learning solutions are being adopted by universities and schools.	Use of blockchain for online education credentials and secure exams	Adoption of AI-powered tools for data-driven teaching and personalized learning
	Growth in cloud collaboration tools for virtual classes and research purposes	Potential adoption of blockchain for digital libraries and resource management	Early-stage use of AI systems for grading and feedback automation
Key Technologies Used	Google Classroom, Microsoft Teams, Zoom, and other cloud platforms	Ethereum, Hyperledger, and public blockchains for data integrity	Machine Learning (ML), Natural Language Processing (NLP), AI-driven analytics
	Use of cloud storage for secure access to learning materials and data	Smart contracts for automated student transactions (admission, certification)	AI-based virtual tutors and learning assistants
Security & Privacy	Focus on cloud security for protecting student data, grades, and curriculum materials	Blockchain provides tamper-proof records of academic achievements	Data privacy concerns around AI algorithms and student profiling
	Government regulations for data sovereignty and secure cloud storage for student records	Blockchain's immutable ledger improves trust in digital academic records	Focus on ethical AI to ensure privacy, transparency, and bias-free learning
Research & Development	Investment in cloud infrastructure for digital learning tools	Exploration of blockchain for student loans, funding, and research integrity	Focus on AI-based education research in personalized learning systems
	Research into cloud solutions for interactive education tools	Use of blockchain for open educational resources and research collaboration	AI-driven research in education technology, learning behavior prediction
Challenges	Limited cloud infrastructure in rural areas for remote learning	Regulatory barriers around blockchain adoption in education	AI bias and challenges in ensuring fairness and transparency in educational systems
	Concerns about data sovereignty and cloud security	Scalability issues and the integration of blockchain into existing education systems	Shortage of AI talent and educators skilled in AI technology

Regional Collaboration	Central Asia collaboration for cloud services in education	Regional partnerships exploring blockchain applications in education	Collaboration with global AI organizations to enhance local AI expertise
	Cloud-based education initiatives in collaboration with international universities	Cross-border collaboration on blockchain for academic certification	AI-based education collaborations in agriculture, healthcare, and digital transformation
Governmental Support	Government is fostering cloud adoption in education through digital transformation plans	Uzbekistan's blockchain strategy includes secure academic records	National AI strategy includes education as a focus area for AI development
	Investment in cloud infrastructure to support digital classrooms and learning resources	Blockchain-based pilot projects are supported by the government to ensure authenticity of student credentials	Government supports the creation of AI research centers in education
Future Outlook (2024)	Cloud-first approach to education, with an increased emphasis on virtual classrooms and e-learning	Blockchain integration will grow, focusing on digital certification and student data management	AI-driven education tools will grow, focusing on personalized learning, student performance tracking, and automated assessment
	Increased investment in cloud infrastructure for nationwide digital education	Blockchain will become a key player in secure academic transactions and digital diploma issuance	Continued rise in AI adoption in education systems for personalized learning experiences

IV. CONCLUSION

Through the use of information technology, it is possible to identify gifted students and create effective, advanced systems to improve their effectiveness. Cloud computing, blockchain, and AI technologies help make the learning process more efficient, transparent, and individualized. At the same time, additional support and investment by the government and educational institutions is needed to further modernize the education system. The use of Information Technology in the identification of students with impotence and the analysis of their effectiveness increases the effectiveness of the educational system and allows teachers to better understand students:

1. More accurate assessment of student effectiveness, optimization of the educational process in innovative ways, AI will help in forecasting the results achieved.
2. Easy monitoring and analysis capabilities to teachers, personalization and special approach, etc. can be implemented through cloud.
3. And blockchain will help in transparency and reform.

The use of Information Technology in identifying gifted students and analyzing their effectiveness helps to implement innovative approaches in the educational system. Through this, it is possible to better measure the effectiveness of students, support them in a personalized way and optimize the educational process. With the help of new technologies, the efficiency, transparency and reliability of the educational system will increase.

V. REFERENCES

1. Sen J., Security and privacy issues in cloud computing //Cloud technology: concepts, methodologies, tools, and applications. – IGI global, 2022. – С. 1585-1630.
2. Modi C., et al. A survey on security issues and solutions at different layers of Cloud computing //The journal of supercomputing. – 2021. – Т. 63. – №. 2. – С. 561-592.
3. Khudoykulov Z., et al. Blockchain Based E-Voting System: Open Issues and Challenges //2021 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2021. – С. 1-5.
4. J. Guo, X. Ding, and W. Wu, "A blockchain-enabled ecosystem for distributed electricity trading in smart city, "IEEE Internet of Things Journal, vol. 8, no. 3, pp. 2040–2050, 2021.
5. Csaky, R. (2019). Deep learning based chat bot models. arxiv preprint arxiv:1908.08835.
6. Karri, S. P. R., & Kumar, B. S. (2020, January). Deep learning techniques for implementation of chat bots. In 2020 International conference on computer communication and informatics (ICCCI) (pp. 1–5). IEEE.
7. Yoo, J., & Cho, Y. (2022). ICSA: Intelligent chat bot security assistant using Text-CNN and multi-phase real-time defence against SNS phishing attacks. Expert Systems with Applications, 207, 117893.

8. Sahoo, S. R., & Gupta, B. B. (2019). Hybrid approach for detection of malicious profiles in twitter. Computers & Electrical Engineering, 76, 65–81.
9. Gupta, B. B., Yadav, K., Razzak, I., Psannis, K., Castiglione, A., & Chang, X. (2021). A novel approach for phishing URLs detection using lexical based machine learning in a real-time environment. Computer Communications, 175, 47–57.