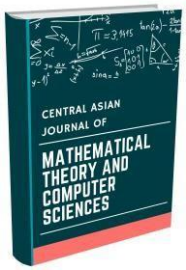

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS
Volume: 06 Issue: 01 | January 2025 ISSN: 2660-5309

Article

An Authentication Approach To Secure And Validation To Access A Big Data In Clouds

Khalid Khalis Ibrahim[1], Luay Ibrahim Khalaf[2], Shihab Ahmed Hmadi[3]

1. Department of Computer Science, College of Computer Science and Mathematics, Tikrit University, Tikrit, Iraq.
2. Department of Computer Science, College of Computer Science and Mathematics, Tikrit University, Tikrit, Iraq.
3. Department of Computer Science, College of Computer Science and Mathematics, Tikrit University, Tikrit, Iraq.

* Correspondence: khalid.kh.ibrahim@tu.edu.iq, luay.i.khalaf@tu.edu.iq, shihab.a.hamddi@tu.edu.iq

Abstract: The protection of large IT systems is a challenging and an interesting area of problem solving in the realm of internet of things (IoT). There is a wide variety of methods that can be implemented to attack and disrupt the transmission of signals in IT systems, for example, data interception. As a result of such attacks, attackers can gain access to the data being transmitted to and from an IT system. This can be achieved by encryption and decrypting, an encoded language that neither computer nor human can understand. Ccounteracting this attack, this paper suggests an access framework that addresses the issue of data access in an attack and analyzes its security and efficiency. The main advantages of this framework include the ability of the data owner to rightfully validation and authentication the details of an unknown user accessing data and the ability to validation information given by other users for message signal recovery (and hence, avoid attacks on such IT systems). After the framework is explained in the realm of data access through an experiment.

Keywords: Authentication, Big data, Internet of things (IoT), Security validation

Citation: Ibrahim K. K. An Authentication Approach To Secure And Validation To Access A Big Data In Clouds. Central Asian Journal of Mathematical Theory and Computer Sciences 2025, 6(1), 17-25.

Received: 10th Jan 2025
Revised: 11th Jan 2025
Accepted: 24th Jan 2025
Published: 25th Jan 2025

1. Introduction

In the 21st century world, data transmission involves large volumes of data being transmitted simultaneously. Big data simply means using predictive analytics, user behavior analytics, or similar, efficient data analytics methods that seldom to a particular size of data set [1]. Due to the numerous information-sensing IoT devices collecting and transmitting data, stored data grows rapidly. Examples of such devices include aerial devices (remote sensing), software logs, cameras, microphones, radio-frequency identification (RFID) readers and, generally speaking, IoT [2]. To avoid any collapse in transmission, developed processing techniques are required to enable improved data access decision making and efficiency. Cloud servers are commonly used to store large data outsourced from data owners and effectively process user access requests to the stored data, but discrete information may be uncovered, which is why cipher text of the data is stored in the cloud instead. Another disadvantage of cloud servers is that it is a highly popular method of secure data storage, which makes it even more difficult to provide an effectively managed access policy to ensure data security [3]. Finally, another

posed issue is figuring out the legitimacy of users requesting outsourced data in cloud servers.

When analyzing IoT implemented in IT systems in terms of power constraints, there are limitations on storage and processing operations, like limited available energy, communication range, bandwidth, etc., which can lead to such systems being open for attacks like eavesdropping and data theft [4]. Hence, many methods have been proposed in the past to overcome these issues, like early ID-based cryptography, which generates a unique ID from a user's mobile phone number, email address, etc., and a private key generator assigns associated individual keys for each user [5]. Another good example developed early this century is an integration identification framework that compresses multiple identifications generated by different users on different messages into a single short, integrated identification. The identification's validity can is matched with every other identification validity, thus creating the integrated identification. Essentially, the integrated identification is valid only if each individual user requesting data access signed its own message [6].

2. Materials and Methods

Many different user models have been suggested by researchers and developers in the past. Here is a fine example in this experiment, the cloud security risks and threats of three different cloud service models were compared by including real world cloud attacks to describe in detail the methods that attackers use against cloud servers. Also, various techniques to prevent cloud security breaches are presented [7]. Another study discusses some of the critical security issues through various aspects of cloud servers. This study also aims to explain some network concerns to stagnate the threats inside clouds, researchers, CSP (Cloud Service Provider) and end users for a proper analysis of the threats [8]. A recent paper suggested a method that provides several advantages like enhanced detection of harmful software, forensics capabilities and operation execution. A lightweight, cross-storage host agent and a network service are involved in the execution of this method. The method combines detection methods, static identifications analysis and dynamic analysis detection. Through experiments with this method, it is discovered that cloud-based malware detection provides 35Our work is a Systematic Mapping where we hope to present metrics about publications available in literature that deal with some of the seven security threats in Cloud Computing, based in the guide Top Threats to Cloud Computing" from the Cloud Security Alliance (CSA). In our research we identified the more explored threats, distributed the results between fifteen Security Domains and identified the types of solutions proposed for the threats. In face of those results, we highlight the publications that are concerned to fulfill some standard of compliance [10]. Another paper presents the current threats to the cloud environment, and then a multiple detection system that is used to tackling the spread of malware throughout the cloud server [11].

The most critical security attacks in cloud computing are covered in another paper, which proposes relevant solutions to strengthen security within a cloud server. In addition to that, secure cloud architectures for different organizations to modify the security of cloud servers are suggested and described [12]. Finally, in another release, the authors propose a layout to design a quality management system (QMS) of CCSs, proactive digital forensic (DF), proactive and predictive security controls and corporate DF investigation methods up to the level specified in the Service Level Agreement (SLA) [13].

Proposed Methods

Before jumping into the proposed method for the first experiment, it is important to briefly review what cloud servers are they can be classified into two main categories. First, public clouds in which the data storing and accessing environment is shared between multiple users, and second, private clouds with are meant only for a single user. Applications that implement cloud servers require data to be stored in cipher text and access requests by one user are validated by other users in a given server. As mentioned

earlier, to overcome the vulnerabilities of networks implemented in IT systems, an experiment is conducted. In this experiment, detection of malware, (i.e., software bugs placed through data access for extraction) is performed through a quality management system, proactive digital forensic along with a self-investigation process, and proactive and predictive security controls. A secure access control framework is suggested and explained in this paper, and the following challenges are dealt with – securely storing data in a cloud server and distributing the access rights to all legitimate users, confirming the legitimacy of a user for accessing the data, recovering the original plaintext (i.e., not cipher text) data when the access rights are granted to a user by other users and efficiently modifying the stored cipher text in the cloud when the access policy of the data is changed by the data owner. Most charts graphs and tables are one column wide (3 1/2 inches or 21 picas) or two-column width (7 1/16 inches, 43 picas wide). We recommend that you avoid sizing figures less than one column wide, as extreme enlargements may distort your images and result in poor reproduction. Therefore, it is better if the image is slightly larger, as a minor reduction in size should not have an adverse affect the quality of the image.

3. Results

The following flow chart depicts the secure access framework used in the first experiment. The following flow chart depicts the secure access framework used in the first experiment.

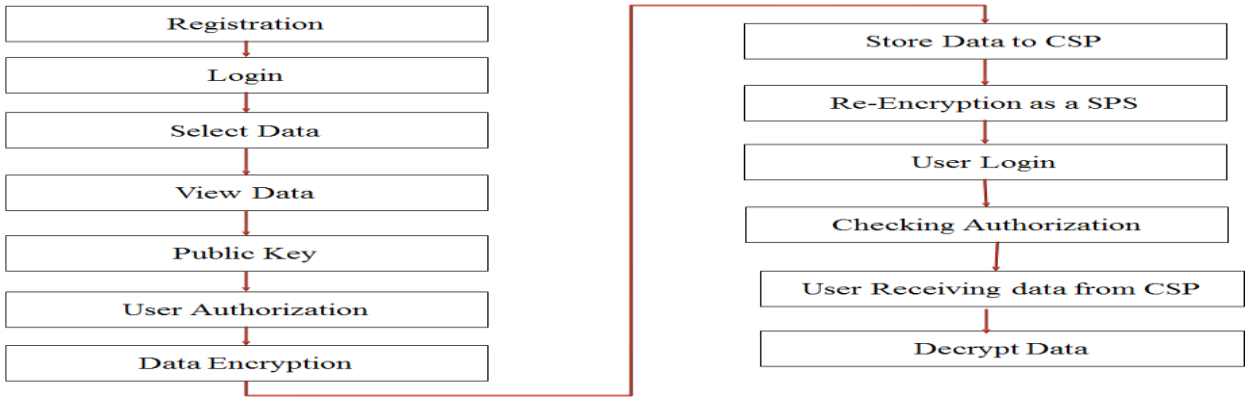

Figure 1. Flow chart for secure access framework

The entire framework consists of five phases that are executed in the following sequence:

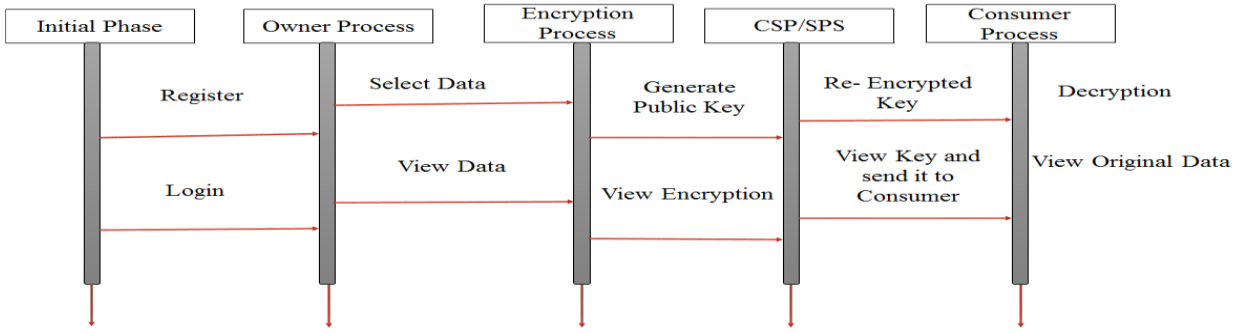

Figure 2. Sequence diagram for secure access framework

The steps taken in each of these phases in figure 2 are described below:

a) Initial Phase

* The login process for a user is performed (if it's a new user requesting data, the user goes through the registration process, enter their information into the database and be assigned a cloud ID) see figure 3.

*After logging in, the data is transferred in a proper way.

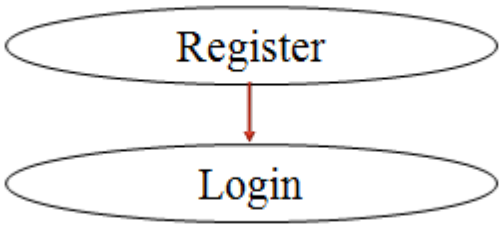

Figure 3. Initial phase flow chart

b) Owner Process

* The owner of the data needs to select the data to be transferred and it can take any format (for pdf, ppt or doc files, the data is converted into text format).
* It is then encrypted, see figure 4.

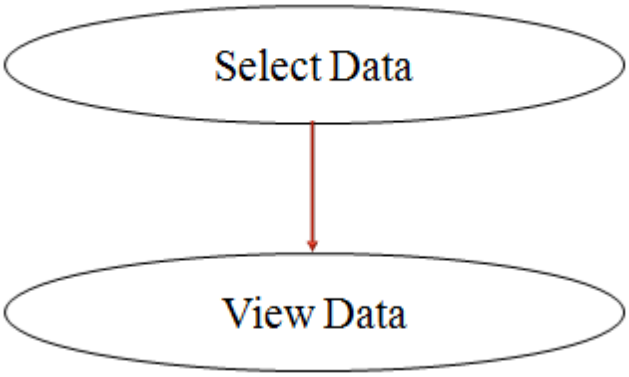

Figure 4. Owner process flow chart

c) Encryption Process

*The data owner generates the message authentication code for the data to be transferred, The MAC (medium access control) framework is used as the key for the encryption of the data and after that to encryption, the Data Encryption Standard algorithm (DES) is used and it uses 56 bits as a key size.

* The data owner sends the authorization rules, which contain the names of the receivers with authorization, see figure 5.

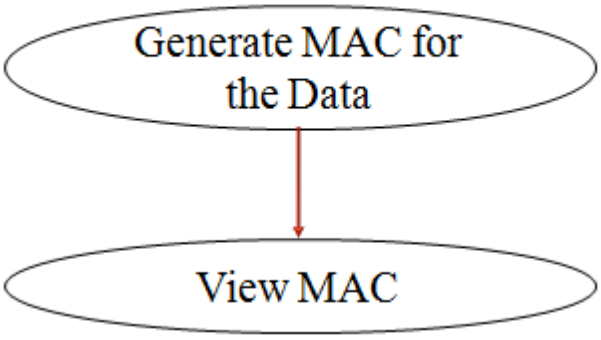

Figure 5. Encryption process flow chart

d) Re-Encryption keys.

*Using the re-encryption key, the encrypted data must be encrypted again.

* Cloud service provider then receives the request from data user, see figure 6.

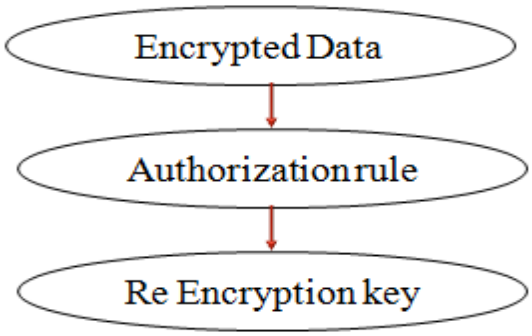

Figure 6. Cloud Service Provider flow chart

e) Consumer Process

The data user has to login into the system and send a request to the CSP, The CSP validates the request from the data user, using the authorization rules, If the data user name is present in the authorization rules means the CSP will provide the If the data is provided, the user decrypts it , see figure 7.

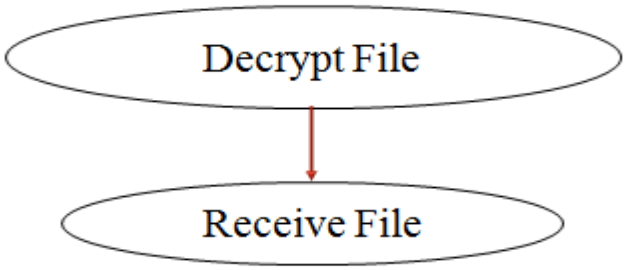

Figure 7. Consumer process flow chart

In this experiment an arbitrary user first performs the initial phase, owner process and encryption process. Once that is done, the CSP automatically decrypts the encrypted and received data. After that, two users send requests to the CSP to access specific data (after logging into the server themselves), the associated authorizations are determined by the CSP. If the two users are authorized, the CSP sends them the encrypted (again) requested data in encrypted form, which then the users must decrypt once received. The following flow chart depicts the events of this experiment see figure 8.

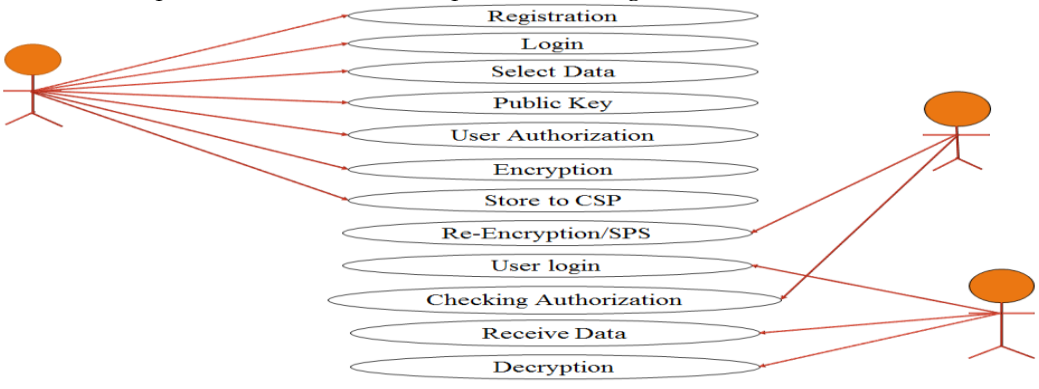

Figure 8. Experiment Test Flow Chart

4. Discussion

For the first experiment, the described flow process from the previous section is executed using the following user designed GUIs (Graphical User Interfaces) see figure 9 were implemented with each step of the process: The above figure 9 represents what information a new user would have to enter to join the cloud network. The data collected through each of these text fields gets encrypted into cipher text before it is transmitted to the data center for validation. Once received by the data center, it is decrypted see figure 10.

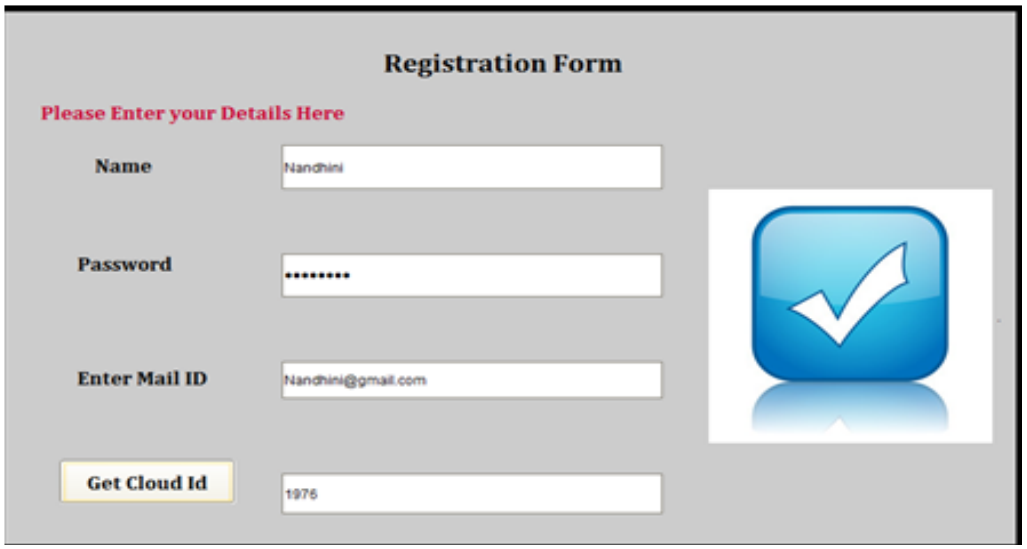

Figure 9. GUI for the Initial Phase of the framework

Figure 10. GUI for the Owner Phase of the framework

In the figure 10 above, the owner can browse through his/her files, select which ones to send to the cloud server and upload them accordingly. The owner also has the option to open various folders and browse through them on the GUI itself, and more importantly, view the file as well before uploading it.

Figure 11. GUI for the Encryption Phase of the framework

In the figure 11 above, the data owner can encrypt the file before sending it off to the cloud server. Along with that, the owner can view the associated re-encryption key for other users to gain access and can also perform a validation of the current authorized users of the data.

Figure 12. GUI for the Cloud Server Provider phase of the framework

In the figure 12 above, the GUI is used by the Cloud Server Provider to perform its tasks for data owners and users. The CSP receives the data that was transmitted from the data owner, along with the associated key. It can also view the encrypted version of the data being dealt with at the moment.

A consumer or user that is authorized to access data by the owner eventually received the required data through a GUI like or even identical to the one shown in the figure 13 below. The user does need to decrypt the incoming data from the cloud server before being able to read it, hence the GUI does provide those options.

The experiment, described so far to test the validation and authentication framework and compare it with the older framework, can be performed multiple times to test for average efficiency.

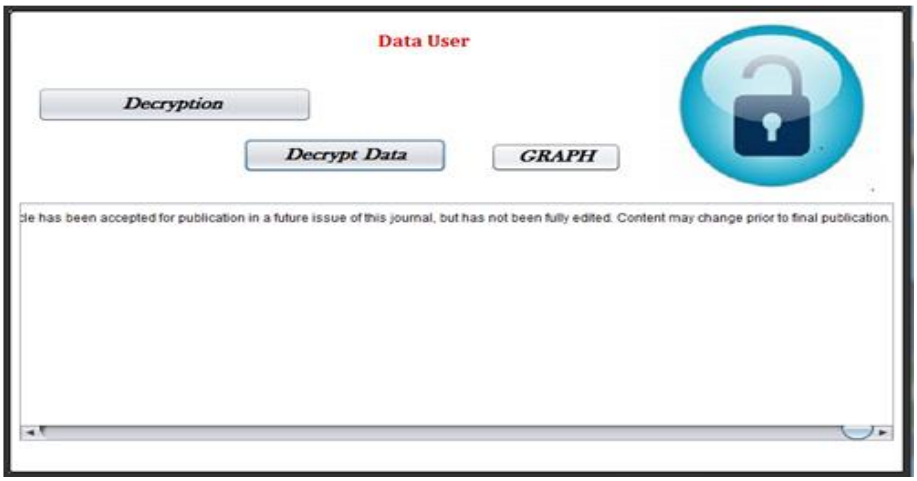

Figure 13. GUI for the Consumer phase of the framework

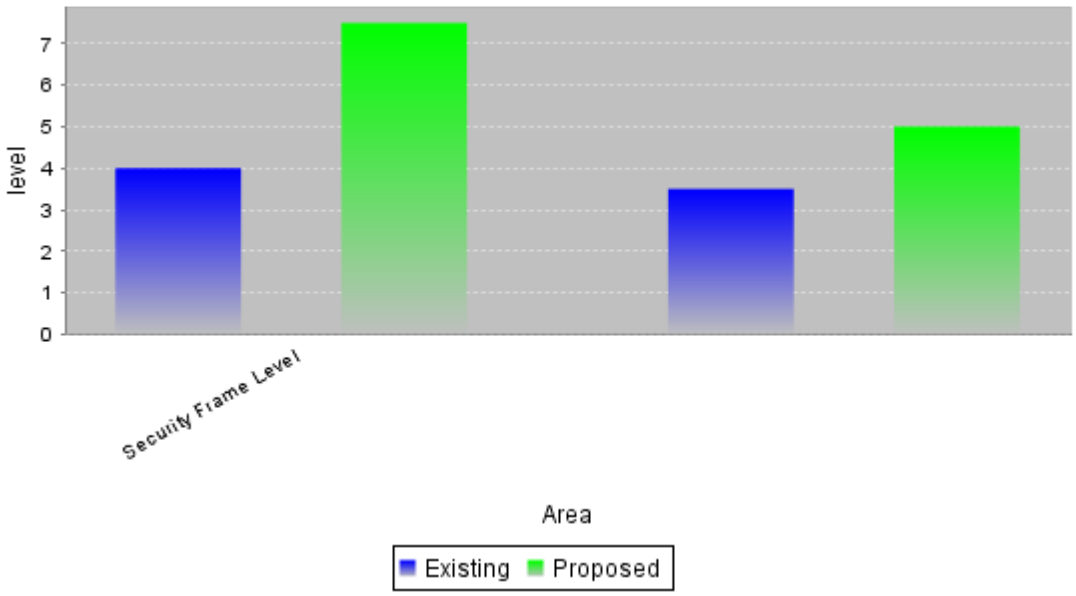

Figure 14. Bar graph depicting the security level for networks of different areas using both the original Identification based framework and the validation and authentication framework.

The figure 14 above depicts the results of two experiments, hence testing the two frameworks on two different randomized networks each. Each network has a different area, and the results of the two frameworks are compared in terms of security level.

5. Conclusion

From the experiment that was conducted to test the efficiency of the suggested framework at combating data security threats, many positive conclusions can be drawn. The suggested framework allows a data owner in the cloud server to dynamically update his/her data access policy. On top of that, the framework proves to provide accuracy in data output from transactions between different components of the network, stable security and computational efficiency (especially considering complexity of the algorithms involved).

REFERENCES

[1] R. Simon, *Results of the Data Analysis Army Aircrew Coordination Measures Testbed Conducted Conducted Spring 1990*. 2001. doi: 10.21236/ada398687.

[2] O. Brovkina and S. Baranova, "Family vs Discourse," *PSYCHOLINGUISTICS*, vol. 25, no. 2, pp. 31–49, Apr. 2019, doi: 10.31470/2309-1797-2019-25-2-31-49.

[3] N. Muradullayeva, "SAMARQAND VILOYATIDA MAISHIY XIZMAT KO'RSATISH SOHASINI SAMARADORLIGINI BOSHQARISH OMILLARI," *Nashrlar*, pp. 337–340, Oct. 2023, doi: 10.60078/2023-vol1-iss1-pp337-340.

[4] D. Tasche, "Bayesian estimation of probabilities of default for low default portfolios," *Journal of Risk Management in Financial Institutions*, vol. 6, no. 3, p. 302, Jul. 2013, doi: 10.69554/zfgq4746.

[5] A. K. Alikulovich and Z. Tulkinova, "DEVELOPMENT STRATEGY OF NEW UZBEKISTAN FOR 2022-2026," *The American Journal of Social Science and Education Innovations*, vol. 05, no. 05, pp. 5–9, May 2023, doi: 10.37547/tajssei/volume05issue05-02.

[6] D. Lando and T. M. Skødeberg, "Analyzing rating transitions and rating drift with continuous observations," *Journal of Banking & Finance*, vol. 26, no. 2–3, pp. 423–444, Mar. 2002, doi: 10.1016/s0378-4266(01)00228-x.