UDC 004.93

DESIGN AND EVALUATION OF AN SVM-BASED BIOMETRIC AUTHENTICATION SYSTEM USING KEYSTROKE DYNAMICS

[1]Rasulmukhamedov M.M.,[2]Mirzaeva G.R., +[3]Gafforov N.Y.

+mrgaffarov28@gmail.com
[1]Tashkent State Transport University,
[2]Tashkent University of Information Technologies named after Muhammad al-Khwarizmi,
[3]Research Institute for the Development of Digital Technologies and Artificial Intelligence

Annotation: This study considers the issues of creating a biometric authentication system based on the dynamics of keystrokes and improving its efficiency. Since traditional password-based authentication methods are not sufficiently reliable from a security perspective, a biometric authentication method based on the analysis of users' keyboard typing habits is proposed. The study uses the Support Vector Machines (SVM) model to analyze and classify user typing patterns. An authentication system is developed based on keystroke force and latency data, and its False Rejection Rate (FRR) and False Acceptance Rate (FAR) indicators are evaluated. The results obtained demonstrate the efficiency of the authentication system based on the dynamics of keystrokes using the SVM model. The results of the study pave the way for exploring the possibilities of integrating keyboard biometrics with other authentication methods in the future.

Keywords: Biometric authentication, keystroke dynamics, Support Vector Machines (SVM), user identification, machine learning, FRR, FAR, security, latency, pressure force.

1 Introduction

As information technology advances, the protection of personal and corporate data is becoming increasingly important [1]. Traditional authentication methods, including passwords and PINs, are not sufficiently reliable from a security perspective. Since they are easy to hack or steal, there is a growing need for alternative authentication methods, especially biometric technologies [2].Biometric authentication systems are based on a person's unique physiological or behavioral characteristics, and their level of security is much higher than traditional methods [3]. For example, methods such as fingerprint, facial recognition, and voice authentication are widely used in identity verification. At the same time, Keystroke Dynamics, an authentication method based on the analysis of the user's typing habits on the keyboard, is also showing high efficiency.

Keyboard dynamics is based on the principle that each person's typing style is unique. Each user types on a keyboard at a different speed, presses different keys differently, and uses different amounts of force. These characteristics create a user's unique typing pattern, which can be a powerful biometric indicator for authentication. The keystroke dynamics authentication system analyzes specific patterns in the user's password typing process and uses them for identification purposes. In this method, the dynamics of each keystroke performed by the user - the pressure force, the duration of the keystroke, and the delay time between letters - are taken into account. As a result, the system learns the user's individual behavior and uses them in future authentication processes.

The keystroke dynamics authentication system analyzes specific patterns in the user's password typing process and uses them for identification purposes. In this method, the dynamics of each keystroke performed by the user - the pressure force, the duration of the keystroke, and the delay time between letters - are taken into account. As a result, the system learns the user's individual behavior and uses them in future authentication processes. Using machine learning algorithms such as Support Vector Machines (SVM) in keystroke-based authentication systems can improve performance. SVMs can classify user typing patterns and help assess whether new input is valid or invalid. This reduces the likelihood of false authentication.

This paper analyzes the implementation of a keystroke dynamic authentication system using SVM. The results of the research are aimed at determining the effectiveness of this approach compared to traditional authentication methods. This will serve to increase cybersecurity and expand the possibilities of protecting users' personal information. The authentication system based on the dynamics of keystrokes can be used in various fields in the future, including banking systems, government institutions, and special security systems. The convenience and high level of security of this method make it a promising technology to replace traditional authentication methods.

2 Literature review

Many studies have been devoted to developing authentication systems based on keyboard typing dynamics. This method has proven to be effective in identifying individual user typing habits and strengthening security systems [4]. A study by Wahyudi Martono, Hasimah Ali, and Momoh Jimoh E. Salami examined methods for identifying users based on the difference in keystroke timing. The study used the Support Vector Machines (SVM) algorithm, which was reported to have high accuracy in the authentication process [5]. Previous studies have proposed fuzzy logic-based authentication methods, such as those proposed by William and De Jan (1997). This method analyzes the dynamics of different keystroke patterns and identifies typical typing styles of users. However, as the flexibility of fuzzy logic systems increases, so does their complexity [6].

In research conducted by Lin (1997), a methodology for learning keyboard typing patterns using neural networks was developed. Although this method was quite flexible, it had problems when working with large amounts of data [7]. In recent years, Zhang (2000) has conducted research on automated authentication systems based on keyboard biometrics. This study analyzed the typing patterns of different users and explored the possibilities of creating individual profiles [8]. Currently, authentication systems based on keystroke dynamics have been proven to provide a higher level of security than traditional passwords. In particular, the use of machine learning algorithms such as SVM and artificial neural networks is helping to increase the accuracy of the system. In the future, research in this area will further develop, allowing the development of more accurate and efficient authentication systems.

The system considered in this paper, unlike the methods used in other studies, includes two main features, keystroke pressure and latency. This method can achieve high accuracy using SVM and significantly reduce the FRR and FAR indicators. Keystroke Pressure – Indicates the amount of force the user applies when pressing keys on the keyboard. This information can be obtained on touch keyboards or special pressure-sensitive keyboards. This feature is used to identify individual actions.

Latency – The time difference between key presses.

- Flight time – the time it takes to move from one key to the next.
- Dwell time – the duration of a key press (how long it is pressed).

The above literature review shows that various methods have been tested to improve the efficiency of authentication systems based on the dynamics of key presses. The SVM model is a promising technology for this purpose, and its further development will serve to increase the security level of authentication systems.

3 Research methodology

3.1 The problem is posed

The main challenge in this research is to identify individuals based on the dynamics of keystrokes and increase the accuracy of the authentication system. Traditional passwords can be easily cracked, so the aim is to strengthen the authentication process by evaluating users' typing habits [9].Since users' typing styles are individual, analyzing the unique characteristics of keyboard pressure force and typing speed can be effective in the authentication process. Therefore, the research aims to explore ways to strengthen traditional password systems by using keyboard dynamic biometrics. The main objective of the study is to develop a biometric authentication system based on the dynamics of

keystrokes and classify them using Support Vector Machines (SVM). During the study, the characteristics of the users' typing styles were recorded and their pressure and time interval data were analyzed.

In addition, the study calculated metrics such as False Rejection Rate (FRR) and False Acceptance Rate (FAR) to assess the reliability of the authentication system. The possibility of using various machine learning models to improve the system was also considered. The research results show that an authentication system based on the dynamics of keystrokes can provide a higher level of protection than traditional methods. This approach can be used especially in systems that require a high level of security. Future research will focus on creating personalized models and developing flexible authentication mechanisms for users, and will also explore the possibilities of further improving the SVM algorithm and comparing it with neural networks.

3.2 Solution methods

During the research, Support Vector Machines (SVM) classifier was chosen as the basis for creating an authentication system [10]. The SVM algorithm studies the dynamics of user keystrokes and determines the optimal classification threshold based on them. This method serves to evaluate user typing patterns and reduce the probability of false rejection or acceptance during the authentication process.

In the first stage, data on the user's typing habits is collected. The force and time interval of each keystroke on the keyboard during each user's password entry process are recorded. The time interval is calculated as the time between two consecutive keystrokes and is determined using the following formula:

$$L_{ij} = T_j - T_i \tag{1}$$

where and are the pressed time moments of buttons T_i and T_j, respectively.

In the second step, the pressure applied by the user to each button is determined. This is expressed as the maximum pressure force and is found using the following formula:

$$P_i = \max\left(F_i\right) \tag{2}$$

where – F_i the force generated by the user when pressing the button.

In the next step, the collected feature set is processed using Support Vector Machines (SVM). The SVM classifier works with the following basic optimization formula to determine the optimal hyperplane:

$$w \cdot x + b = 0 \tag{3}$$

where w is the vector of weights, x is the vector of input features, and b is the bias parameter of the model. To determine the optimal classification threshold, SVM is based on the following margin maximization principle:

$$max \frac{2}{w} \tag{4}$$

This allows the authentication system to reduce the probability of false acceptance and rejection. To assess the effectiveness of the authentication process, the False Rejection Rate (FRR) and False Acceptance Rate (FAR) indicators are calculated:

$$FRR = \frac{N_{FR}}{N_{AA}} \times 100\% \tag{5}$$

$$FAR = \frac{N_{FA}}{N_{IA}} \times 100\% \tag{6}$$

where N_{FR} is the number of falsely denied cases, N_{FA} is the number of falsely accepted cases, N_{AA} is the number of authorized user attempts, and N_{IA} is the number of illegal login attempts.

This method can make the authentication system more reliable and reduce the possibility of misclassification. According to the results of the study, a biometric authentication system based on the dynamics of keystrokes has a security advantage over traditional passwords.

4 Analysis and discussion of results

The results of the study were aimed at evaluating the effectiveness of a biometric authentication system based on the dynamics of keystrokes [11]. During the experiment, a group of 5 users was selected and the typing habits of each user were recorded. Each user entered a 6-character password 200 times, 100 of which were used for training the model and the remaining 100 for testing.

The following table shows the False Rejection Rate (FRR) and False Acceptance Rate (FAR) results:

Table 1. False Rejection Rate (FRR) and False Acceptance Rate (FAR) results

User	FRR (%)	FAR (Closed set) (%)	FAR (Open set) (%)
User_1	2	0	10
User_2	7	1.75	14
User_3	19	0.5	1.5
User_4	0	0.75	0
User_5	0	1.75	48
Average	5.6	0.95	14.7

The results show that the SVM model can improve the efficiency of the authentication system by optimizing the FRR and FAR metrics.

The training and classification times for the SVM model were also evaluated during the study. The following table shows a comparison of the model training and testing times for each user:

Table 2. Comparison of model training and testing times

User	Training time (sec)	Classification rate (%)
User_1	0.0625	100
User_2	0.6563	100
User_3	0.4687	100
User_4	0.6250	100
User_5	0.2815	100
Average	0.4188	100

These results indicate that the SVM model is effective for authentication systems. Future work could include comparing the model with neural networks and testing it with an increasing number of users.

Analysis shows that a biometric authentication system based on keystrokes can provide high-accuracy authentication through a user's typing habits. This method increases security and reduces the likelihood of false acceptance or rejection compared to traditional passwords.

5 Conclusions and suggestions

This study focused on the performance of a biometric authentication system based on keystroke dynamics. The results showed that the SVM model can effectively analyze individual user typing patterns and perform their identification with high accuracy [12]. According to the experimental results, the average FRR was 5.6% and the FAR was 0.95% for the closed set. These results indicate that the proposed system can be more secure and reliable than traditional password-based authentication methods. In order to further improve the efficiency of the system in the future, the following suggestions are put forward. First, the accuracy indicators can be increased by applying Deep Learning approaches to the model. Second, the study should be conducted with the participation of more users, since the collection of more data improves the generalization ability of the model. Third, lightweight and optimized algorithms should be introduced to further speed up the authentication process.

The system can also be integrated with other biometric authentication methods, such as facial recognition or fingerprint authentication, which increases security and makes the authentication process more reliable. The results show that a biometric authentication system based on keystroke dynamics can be used as an alternative to traditional password systems. It helps to ensure a high level of security and ease of use, while preventing unauthorized access by analyzing individual user behavior [13].

References

[1] Eltahir, W.E., Lai, W.K., Salami, M.J.E., Ismail, A.F.: Design of a pressure-based typing biometric authentication system. In: Proceeding of the 8th Australian and New Zealand intelligent information system conference anziis, Sydney AU (2003)

[2] Lin, D.T.: Computer-access authentication with neural network-based keystroke identity verification. In: Proceeding International Conference on Neural Networks, Houston, Texas, USA, pp. 174–178 (1997)

[3] Ilonen, J.: Keystroke dynamics. in: Advanced topics in information processing – lecture (2003)

[4] Burges, C.J.C.: A Tutorial on Support Vector Machines for Pattern Recognition. Data Mining and Knowledge Discovery 2(2), 121–167 (1998)

[5] Wahyudi Martono, Hasimah Ali, Momoh Jimoh E. Salami. (2020). Keystroke pressure-based typing biometrics authentication system using support vector machines. Journal of Computer Science, 16(5), 85-93.

[6] William, G., De Jan, H.P.: Noravshan mantiq asosida kengaytirilgan parol autentifikatsiyasi. IEEE Expert 12(6), 38–45 (1997)

[7] Lin, D.T.: Computer-access authentication with neural network-based keystroke identity verification. In: Proceeding International Conference on Neural Networks, Houston, Texas, USA, pp. 174–178 (1997)

[8] Zhang, D.: Avtomatlashtirilgan biometrik texnologiyalar va tizim. Kluwer academic publishers, Dordrecht (2000), Lan:eng.

[9] Ali, H., Wahyudi, Salami, M.J.E.: Sun'iy neyron tarmog'idan foydalangan holda klaviatura bosimiga asoslangan yozish biometrik autentifikatsiya tizimi. In: Proceeding 1st International Conference on Control, Instrumentation and Mechatronics Engineering, Johor Bahru, Malaysia, pp. 407–412 (2007), Lan:eng.

[10] Cristianini, N., Shawe, T.J.: An introduction to Support Vector Machine and other kernelbased learning methods. Cambridge University Press, Cambridge (2000)

[11] Revett, K., de Magalhaes, S.T., de Souza Tenorio, L. (2008). Evaluating the Stability of Keystroke Dynamics Features. 10th International Conference on Information Security and Cryptology.

[12] Campisi, P. (2013). Security and Privacy in Biometrics. Springer Science & Business Media.

[13] Liu, J., Silverstein, M., Martin, T. (2018). Deep Learning for Keystroke Dynamics-Based Authentication. IEEE Transactions on Neural Networks and Learning Systems, 29(6), 57-68.

РАЗРАБОТКА И ОЦЕНКА СИСТЕМЫ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ SVM С ИСПОЛЬЗОВАНИЕМ ДИНАМИКИ НАЖАТИЯ КЛАВИШ

[1] *Расулмухамедов М.М.,[2] Мирзаева Г.Р., +[3] Гаффаров Н.Ю.*

+mrgaffarov28@gmail.com
[1] Ташкентский государственный транспортный университет,
[2] Ташкентский университет информационных технологий имени Мухаммада аль-Хорезми,
[3] НИИ развития цифровых технологий и искусственного интеллекта

Аннотация: В данном исследовании рассматриваются вопросы создания системы биометрической аутентификации на основе динамики нажатия клавиш и повышения её эффективности. Поскольку традиционные методы аутентификации на основе паролей недостаточно надёжны с точки зрения безопасности, предлагается биометрический метод аутентификации, основанный на анализе привычек пользователя при наборе текста на клавиатуре. В исследовании используется модель опорных векторов (Support Vector Machines, SVM) для анализа и классификации особенностей набора текста пользователей. На основе данных о силе нажатия клавиш и задержках между ними разработана система аутентификации, а также оценены показатели False Rejection Rate (FRR) и False Acceptance Rate (FAR). Полученные результаты демонстрируют эффективность системы аутентификации на основе динамики нажатия клавиш с использованием модели SVM. Итоги исследования открывают возможности для последующей интеграции клавиатурной биометрии с другими методами аутентификации в будущем.

Ключевые слова: биометрическая аутентификация, динамика нажатия клавиш, Support Vector Machines (SVM), идентификация пользователя, машинное обучение, FRR, FAR, безопасность, задержка, сила нажатия.

KLAVIATURA BOSISH DINAMIKASI YORDAMIDA SVM-GA ASOSLANGAN BIOMETRIK AUTENTIFIKATSIYA TIZIMINI LOYIHALASH VA BAHOLASH

[1]*Rasulmuhamedov M.M.,[2]Mirzaeva G.R., +[3]G‘afforov N.Y.*

+mrgaffarov28@gmail.com
[1]Toshkent davlat transport universiteti,Transportda axborot tizimlari va texnologiyalari kafedra mudiri.
[2]Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti,
Dasturlash texnologiyalari kafedra dotsenti.
[3]Raqamli texnologiyalar va sun’iy intellektni rivojlantirish ilmiy-tadqiqot instituti,
Tayanch doktoranti.

Annotatsiya: Ushbu tadqiqot klaviatura tugmalarini bosish dinamikasiga asoslangan biometrik autentifikatsiya tizimini yaratish va uning samaradorligini oshirish masalalarini ko‘rib chiqadi. An’anaviy parolga asoslangan autentifikatsiya usullari xavfsizlik nuqtai nazaridan yetarlicha ishonchli bo‘lmagani sababli, foydalanuvchilarning klaviaturada matn terish odatlarini tahlil qilishga asoslangan biometrik autentifikatsiya usuli taklif etiladi. Tadqiqotda foydalanuvchilarning terish namunalarini tahlil qilish va tasniflash uchun qo‘llab-quvvatlovchi vektor mashinalari (Support Vector Machines — SVM) modeli ishlatiladi. Tugmalarni bosish kuchi va kechikish vaqtiga oid ma’lumotlar asosida autentifikatsiya tizimi ishlab chiqilgan hamda uning FRR (False Rejection Rate — noto‘g‘ri rad etish darajasi) va FAR (False Acceptance Rate — noto‘g‘ri qabul qilish darajasi) ko‘rsatkichlari baholangan. Olingan natijalar tugma bosish dinamikasiga asoslangan va SVM modelidan foydalangan autentifikatsiya tizimining samarali ekanligini ko‘rsatadi. Tadqiqot natijalari kelajakda klaviatura biometrikasini boshqa autentifikatsiya usullari bilan integratsiya qilish imkoniyatlarini o‘rganishga zamin yaratadi.

Kalit so‘zlar: biometrik autentifikatsiya, tugma bosish dinamikasi, Support Vector Machines (SVM), foydalanuvchini identifikatsiya qilish, mashinaviy o‘qitish, FRR, FAR, xavfsizlik, kechikish, bosim kuchi.