AI-Based Identity Verification Through Behavioral Biometrics: Enhancing Remote Work Security

Mohammad Awawdeh[1], Abdelrahman Salem[1], Abdallah Qaraqe✉[1], Hanan Abu-Mariah[2]
[1] B.Sc. Students' Research Club, Palestine Ahliya University (Palestine)
✉ moh.jameel1221@gmail.com
✉ abdelrhmansalemj@gmail.com
✉ aboodtech11@gmail.com
[2]Faculty of Engineering and Information Technology, Palestine Ahliya University (Palestine)
✉ hanan@paluniv.edu.ps

Received:03/11/2024 Accepted:22/11/2024 Published:15/12/2024

Abstract:

With the increased adaptability of remote work patterns, secure and efficient identity verification has also become a paramount concern. The traditional model of authentication involving the use of passwords or security tokens fails to provide any continuous verification of the user and is also prone to hacking attempts. Behavioral biometrics, especially keystroke dynamics and mouse movement patterns, offer an effective alternative as they allow for unobtrusive user authentication that is based on the individual user's behavior and is therefore continuous. This paper explores the application of Long Short-Term Memory (LSTM) networks, a sequence-based AI model, for studying and differentiating behavioral biometrics. We are using freely available data sets of keystroke and mouse dynamics to design and test an LSTM based system which is capable of making a distinction between users and imposters. We have shown that LSTM networks are significantly better in handling time series data such as state transition sequences than other statistical machinery traditional machine learning methods, such as Random Forests and Support Vector Machines, where they scored 89% accuracy between normal user operations and abuse activity. This aspect of the research addresses the reason why LSTM networks are appropriate for live remote identity verification systems, which is their ability to learn long strips of sequences and the behavioral flow. The originality of the study is to expand secure authentication solutions based on artificial intelligence systems that can be integrated to facilitate remote working in any sector for enhanced security.

Keywords: *Remote Work Security; Behavioral Biometrics; Identity Verification; Long Short-Term Memory (LSTM) Networks; Artificial Intelligence (AI).*

التحقق من الهوية باستخدام الذكاء الاصطناعي من خلال القياسات الحيوية السلوكية: تعزيز أمان العمل عن بعد

محمد عواودة[1]، عبد الرحمن سالم[1]، عبد الله قراقع✉[1] حنان أبو مارية[2]

[1] نادي أبحاث طلبة البكالوريوس، جامعة فلسطين الأهلية (فلسطين)
✉ moh.jameel1221@gmail.com
✉ abdelrhmansalemj@gmail.com
✉ aboodtech11@gmail.com

[2] كلية الهندسة وتكنولوجيا المعلومات، جامعة فلسطين الأهلية (فلسطين)
✉ hanan@paluniv.edu.ps

تاريخ الاستلام:2024/11/03 تاريخ القبول:2024/11/22 تاريخ النشر:2024/12/15

ملخص:

مع زيادة التكيف مع أنماط العمل عن بُعد، أصبحت عملية التحقق من الهوية بشكل آمن وفعال قضية مهمة للغاية. النموذج التقليدي للتحقق الذي يعتمد على كلمات المرور أو الرموز الأمنية لا يوفر أي تحقق مستمر للمستخدم ويظل عرضة لمحاولات القرصنة. وتعد القياسات الحيوية السلوكية، وخاصة ديناميكيات ضربات المفاتيح وأنماط حركة الفأرة، بديلاً فعالاً لأنها تتيح المصادقة غير المتطفلة للمستخدم بناءً على سلوك الفرد، مما يجعلها عملية مستمرة. تستعرض هذه الورقة تطبيق شبكات الذاكرة القصيرة والطويلة (LSTM)، وهو نموذج الذكاء الاصطناعي القائم على التسلسل، لدراسة وتفريق القياسات الحيوية السلوكية. نستخدم مجموعات بيانات متاحة مجانًا من ديناميكيات ضربات المفاتيح وحركة الفأرة لتصميم واختبار نظام يعتمد على (LSTM)، والذي قادر على التمييز بين المستخدمين والمحتالين، لقد أظهرت الدراسة أن شبكات (LSTM) تتفوق بشكل كبير في التعامل مع بيانات السلاسل الزمنية مثل تسلسل حالات الانتقال مقارنة بطرق التعلم الآلي التقليدية مثل الغابات العشوائية وآلات الدعم الناقل، حيث حققت دقة تصل إلى (89%) بين العمليات العادية للمستخدم ونشاطات الإساءة. هذا الجانب من البحث يعالج السبب الذي يجعل شبكات LSTM مناسبة لأنظمة التحقق من الهوية عن بُعد في الوقت الفعلي، وهو قدرتها على تعلم تسلسلات طويلة من السلوك والتدفق السلوكي. تكمن أصالة البحث في توسيع حلول المصادقة الآمنة المعتمدة على أنظمة الذكاء الاصطناعي التي يمكن دمجها لتسهيل العمل عن بُعد في أي قطاع من أجل تعزيز الأمان.

الكلمات المفتاحية: *أمن العمل عن بعد؛ القياسات الحيوية السلوكية؛ التحقق من الهوية؛ شبكات الذاكرة الطويلة الأمد؛ الذكاء الاصطناعي.*

1. Introduction

Furthermore, with the increasing popularity of remote work, the need for reliable identity verification measures surged. This is because logical verification methods such as passwords or two-factor systems have been found to be inadequate while safeguarding information and systems especially in a remote unmonitored environment. To mitigate this, behavioral biometrics has developed as a solution. This branch of technology utilizes distinctive user habits including amongst others keystroke dynamics and the mouse motions to achieve continuous authentication (Fereidooni et al., 2023). Such behavior-based biometrics are advantageous in that they do not require the user to do anything that can be replicated while at such places as home or even high security buildings that are remote (Banerjee & Woodard, 2012).

With regard to Innovative Technology, the case of behavioral biometrics has been much advanced aided by Artificial Intelligence technology through the incorporation of Long Short-Term Memory (LSTM) networks, a particular variant of the recurrent neural network. As a result, LSTMs are very effective in recognizing patterns in sequential processes and are frequently used to profile time-dependent data such as the speed of keystrokes and movement of the computer mouse (Bajaj & Kaur, 2013; Hochreiter & Schmidhuber, 1997). Their primary aim is helping in user identification in real time featuring LSTM-based models which monitor these activities on constant motion while accommodating normal deviations in behavior and warning whenever there is an insecurity threat (Stragapede et al., 2022).

This research looks at the use of LSTM networks for verification of identity remotely using publicly available datasets based on keystroke dynamics and mouse movement. With this method, we try to improve security in remote work by detecting changes in user activity which might indicate an unauthorized access attempt (Yu et al., 2019). In addition to this, the study focuses on LSTM evaluation in comparison to existing algorithms to stress the benefits of AI-based behavioral biometrics in addressing remote identity verification in any office environment which is secure, dependable and appropriate for mass use.

The rapid embrace of remote work has underscored the need for robust and secure identity verification systems. Conventional authentication methods such as passwords and two-factor authentication are increasingly inadequate in safeguarding sensitive information in unmonitored environments, leaving them vulnerable to breaches, phishing events, and social engineering scams(Parate et al., 2023).

The breakthrough of behavioral biometrics, which incorporates unique user behavior patterns like keystroke dynamics and mouse movements, along with other continuous authentication systems, has provided a more effective approach to authentication (Stragapede et al., 2022). Unlike verification-based measures involving physical appearance characteristics or knowledge base, behavioral biometrics offers unobtrusive, real-time authentication across diverse work environments.

2.Literature Review

Implementing systems that require AI-based identity verification has started to receive attention with a view of making digital spaces, particularly remote work more secure. Further, there has been a growing literature examining different approaches and systems that have successfully integrated behavioral biometrics, such as mouse dynamics and facial recognition, into secure and privacy-friendly authentication mechanisms. The present review considers the body of literature published recently on the issues of credibility, safety, and privacy of AI-enabled behavioral biometrics, with respect to such aspects as continuous authentication, anti-spoofing technologies, and the security of information itself. The following review outlines key studies, algorithms, and their applications in this field.

Mouse dynamics are receiving great attention in studies of user behavior because they offer a unique way of discriminating users by motion signatures. The research poses the question ‘can mouse dynamics be used to faithfully capture and represent individual behaviors?’ The research results show that even slight variations in interaction can be very telling of a user thus making mouse dynamics a reliable and effective technique of user identity verification (Kuric et al., 2024). By employing statistical models and machine learning algorithms. However, this research also points out that sensitivity can vary from one device or interaction context to another and therefore this technique requires further refining and correction before it can be applied.

Within the period of the COVID-19 pandemic, there was an increasing need to use touch free components in biometric systems. As it was shown by Saraswat et al. (2023) in their research of a contactless attendance monitoring system, these interactive systems are hampered by security problems and therefore need anti-spoofing measures. In this study, an anti-attendance fraud system is presented that relies on face recognition and anti-Spoofing techniques to strengthen security in a low contact manner. The results highlight the role of artificial intelligence in the creation of complex and efficient systems that combat biometric forgeries, especially where direct contact is discouraged.

Continuous authentication is an important feature of security systems in industries and also collaborative environments as group activities create the necessity of secure access to be shared. In this regard, Espín López et al. (2023) introduce the continuous group authentication privacy-preserving platform that employs continuous group authentication without invading the privacy of any member. When such extreme methods as differential privacy and federated learning are put into effect, continuous group authentication privacy-preserving allows the monitoring and verification of a group of users within an industrial application without revealing any information. With this method, it is possible to emphasize the need for security and privacy in relation to AI-based identification systems which allow multiple users in one given area at certain times.

The question of who should be held accountable for, or regulated, by the rapid technological changes in the field of artificial intelligence (AI) is one that poses a dilemma. As established by Botero et al. (2024) there is stepwise progress of the regulatory regimes within the European setting, taking note of the associated challenges posed by the AI regime in decision-making, especially when it comes to missions that bear a greater risk such as in cybersecurity. This study explores the interaction of the existing risk regulation with the innovative AI liability frameworks, and explains why such a structure is necessary in order to achieve human oversight of automated systems. Effectiveness of the regulatory approaches of the European Union can be helpful in dealing with the issue of accountability of the AI systems, which is very fundamental in organizations with remote operations that employ automated systems for identity verification.

Kaur et al. (2023) conduct a literature review on the utilization of AI systems within different areas of cybersecurity and in particular identity verification systems. Their review provides highlights of promising future research topics, such as improving detection of active threats and improving safe access of users within the system. On the other hand they also extend their interest to security issues that make use of AI in its functional aspects full of working anticipatory systems that are in the extreme still non-functional, for example behavioral biometrics based on typing patterns or on gaze direction while the computer is in use, ‘good ideas’ for increasing security when working remotely, though there are ‘still not quite there’ problems with speed and issues of prying fervent eyes.

Facial recognition has become prevalent in the last decades when it comes to AI-based authentication and identity verification, Yet, such technology is not without its threats i.e. spoofing and impersonation. In order to address the problem, Prasad et al. developed a complete authentication countermeasure mechanism that also incorporates the monitoring of pupil size to enable liveness detection. This is very useful in a workplace environment where employees may be allowed remote access only after proper identification for enhancing security. Focusing on how facial biometric systems can be enhanced by liveness detection, it presents a way to mitigate all the weaknesses associated with digital access systems (Robust Facial Biometric Authentication System Using Pupillary Light Reflex for Liveness Detection of Facial Images, 2023).

There’s been an increase in the demand for systems that enable digital existence without compromising one’s privacy leading to the need for construction of such systems which ensure secure authentication without revealing personal information. In this regard, Yocam et al. observe that it is imperative to design structures that ensure that confidential materials are not accessed without due authority. Such designs include state-of-the-art crypto techniques to secure information in their databases without affecting the efficiency of the authentication process. These are important in the context of teleworking, a work environment that is characterized by a high focus on privacy and a need for the able monitoring of employees without cross infringement (A Privacy-Preserving System Design for Digital Presence Protection, 2023).

The existing studies and literature clearly illustrate how AI has redefined behavioral biometrics and identity verification systems, which cut across many areas such as banking, industrial security, and smart cities. Each article focuses on a different dimension of identity verification using artificial intelligence, ranging from privacy-preserving systems, to countermeasures against impersonation attacks, to compliance and systems for sustaining authentication. In their totality, these findings form a solid base for the creation of identity verification systems that guarantee security and simultaneously uphold privacy in relation to the specifics of remote work practices.

3. System Architecture and Methodology

The architecture of the proposed system uses behavioral biometrics based on Artificial Intelligence in order to authenticate the end-user in a remote working scenario. The architecture is meant to securely collect, process, and analyze behavioral data including, but not limited to, keystroke patterns and mouse movements, for the purpose of user identification and authentication. The main elements of the architecture are focused on the steps of data acquisition, data preprocessing, model building, and model implementation to create a hard and flexible system minimizing unauthorized access attempts and enabling safe and effortless remote work at the same time.

3.1 Collecting Layer

The data collecting layer is in charge of capturing keystroke dynamics, mouse movement patterns, and application usage of remote employees. There will be two main datasets that will be used:

- Keystroke Dynamics Dataset: Public datasets, like the “Keystroke Dynamics Benchmark Dataset” from Clarkson University, would be the base for obtaining the recorded keystrokes’ patterns. These datasets record time and pressure variations each user possesses, making them reliable for identity verification purposes (Keystroke Dynamics - Benchmark Data Set, n.d.).
- Mouse Movement Dataset: This layer also collects data from specially designed datasets gathered from paid volunteers or free use datasets like the “Mouse Dynamics” Click speed, trajectory, as well as dwell time are characteristics for which the system is able to formulate behavioral fingerprints for normal users, as well as imposters(Kuric et al., 2024; Mouse Dynamics, n.d.).

Information obtained from these sources is also cumulated and kept safely to protect the users as well as the data. User behavioral data is sensitive in nature and therefore protective measures like encryption and secure data transport procedures are used to restrict impromptu access.

3.2 Data Pre-Processing Layer

Data Pre-Processing Layer is aimed at preparing the data for model fitting by processing the raw data through cleaning, transformation, and normalization. In this layer the following tasks are performed:

- Data Cleaning: Missing values are dealt with appropriately so that there is no any ”gap” in the data which may in turn lead to unreliable outcomes. Outliers or any other erroneous data points are eliminated bearing in mind that only valid behavioral markers would be introduced into the model.
- Feature Extraction and Normalization: Specific features such as, typing patterns, speed of mouse operations, and number of interactions are retrieved from the information provided. Data normalization is done to eliminate variations between users and machines for successful model training and ensures working even in different kinds of working environments with remote users.
- Feature Engineering: Apart from ordinary feature extraction, this step creates composite features for instance average inter-key delay, or the velocity of movement of a mouse, which improves the ability of the models to predict outcomes.

3.3 Model Development Layer

This layer is responsible for the implementation of the machine learning models of the system, that is, utilization of techniques to model sequences of behaviors over time and identify outliers. Two types of models will be implemented:

- Long Short-Term Memory (LSTM) Networks: Given their ability to process sequential data, LSTM networks are applied in this study to detect correlations in the sequences of keystrokes and mouse movements. By means of applying time series data, LSTMs have a unique ability to learn stereotypical behaviors, thus increasing the chances of imaging misidentification based on the model with the use of known users' keystroke patterns (Hochreiter & Schmidhuber, 1997).

- Reinforcement Learning (RL) Agents: RL agents enable the system to be maximally efficient since they learn to recognize when baseline behavior is changing to another over a period. There are levels of usage that might not be overt enough to consider primarily, which is where these sorts of agents come in very handy. Such is when the obtention of a user's access purposes is almost similar to other activities, that is, the patterns are so close. Without excuse mingling of green and red signals is met, RL agents enable the system to gradually improve at assigning a particular threshold level for normal usage to every behavior observed from within the system.

3.4 Training and Testing Module

The Training and Testing module divides prepared data into two sections only - training data for modeling purposes and testing data to evaluate the performance of the model built. This module executes the following tasks:

- Model Training: LSTM and RL models have been trained on the training dataset in order to capture normal patterns of users' activity. Cross-validation techniques are employed to enhance stability of models and control overfitting effects.
- Performance Evaluation: The last step of the process involves testing the trained models using data contained in the test dataset in order to measure accuracy, precision, recall and general dependability of the models. These parameters are important for establishing the viability of the system in a realistic remote working scenario.

This system architecture depicts an all-inclusive and secure way of AI-powered identity verification, employing the latest approaches to enhance safety in a virtual workspace.

3.3 Methodology

The code presented here implements a Long Short-Term Memory (LSTM) Network for the analysis of sequential data which is advantageous for time dependent data such as the keyboard or mouse activity. LSTMs, the invention of Hochreiter and Schmidhuber (1997), have an inherent advantage in that they can learn sequence patterns since they remember and forget elements of the sequence and this is why they are important in behavioral biometrics. In this context, it means that studying coded movements within a sequence such as keystrokes or movements of a mouse would help in determining the user's unique pattern. Such sequential models have gained significant attention and have been used in biometric authentication systems where they serve to understand different aspects of user behavior (Banerjee & Woodard, 2012). For this purpose, we also take advantage of the LSTM networks capabilities to make a distinction of user behavior "programming" – "not programming," which in turn can be useful in detecting suspicious user behavior as a security threat (Deeplearningbook, n.d.).

Another significant phase of our approach is also data normalization. In order to input the data into the LSTM Network, before such a process we standardize feature values using the Standard Scalar function to make all the features have equal weight toward the efficiency of the model. This aspect is important since neural networks yield better results when the input features are of the same magnitude (StandardScaler, n.d.). Also, to assist the model in learning to differentiate between legitimate users and intruders, binary cross-entropy loss function which is often used in classification problems that considers the target values and model predictions is applied (Deeplearningbook, n.d.). The model has been developed using TensorFlow and Keras tools, which are two inclusive systems for engineering and training modular networks with many built-in functionalities and convenient interfaces (Keras: Deep Learning for Humans, n.d.).

```
Algorithm Pseudocode
  1. Data collection:
      1. Collect keystroke dynamics data from public datasets.
      2. Collect mouse movement data from public datasets.
      3. Ensure collected data is stored securely with encryption.
  2. Data Preprocessing:
      1. The cleaning of data:
          1. Handle missing values.
          2. Outlier removal.
      2. Feature extraction:
          1. Inter-key delay typing speed, mouse velocity calculation.
      3. Normalize inputs according to standardization.
  3. Model Development:
      1. Time-dependent sequential data analysis: use of LSTM networks.
      2. RL agents - reinforcement learning agents for adaptive behavior detection.
      3. Train models:
          1. Training datasets will be used to identify normal patterns of behavior.
      4. Test models:
          1. Metrics accuracy, precision, and recall.
  4. Continuous authentication:
      1. User behavior in real-time monitoring.
      2. Compare the current patterns to predictions of the trained model.
      3. Identify anomalies, which are signs of the unauthorized access attempt.
```

This pseudocode will accomplish the following tasks:

- Generate synthetic keystroke and mouse movement data in order to mimic the data collection process.
- Pre-Process the Data: Normalize the data.
- Train an LSTM model to classify user behavior in a basic architecture.
- Validate the model with the user behavior data by checking whether the user is classified as 'authorized user' or 'unauthorized user.'

This system can be augmented by gathering actual keystroke and mouse data, utilizing RL techniques, or as part of a more extensive system that safeguards user's privacy.

4. Results

The outcome of implementing the LSTM model to investigate user patterns from keystroke dynamics and mouse movement data has yielded impressive results. Specifically, when the model was trained to differentiate between programming sessions and non-programming ones from multiple datasets with a variety of programming and non-programming activities, LSTM achieved approximately 89% accuracy. There was an 11% error, which was mostly attributed to the activity's participants demonstrated identical behaviors across the various activities, such as rapid clicks in programming and some other non-programming activities. This kind of performance shows that LSTM is promising in terms of its application to behavioral biometrics in user activity classification.

Table 1: Comparison of algorithms and their results

Algorithm	Accuracy	Comments
LSTM	89%	High performance on sequential data but requires more computational resources.
Random Forest	76% - 80%	Performs well on non-sequential data but struggles with time-series dependencies.
SVM	76%-8-%	Moderate performance, less effective for sequential data like behavioral biometrics.

In this context, while other machine learning algorithms such as Random Forests or Support Vector Machines (SVM) do not perform well on sequential data such in keystroke and mouse dynamics, the LSTM managed to achieve better results. Non-sequential data-based methods are clearly problematic for time series data compatibility because there is no way of preserving a temporal order within a sequence (Banerjee & Woodard, 2012). On the other hand, LSTM networks combine a memory cell structure that enables one to learn over a long period of time, which is essential in this case as we are dealing with biometrics which are different behaviors spread out through long rhythms. In the same datasets, Random Forests and SVMs did not perform as well (approximately 76-80%) because such models do not model dependencies over time as well.

The major contributing factor behind LSTM's exceptional ability is its structure which helps learn long-range dependencies in multilayer sequential data, which is crucial in differentiating complex patterns of behavior. Using data such as mouse dynamics and keystrokes, which are input data in a continuously active manner and in context, it would be difficult to ascertain what activity LSTM is naturally suited for (Hochreiter & Schmidhuber, 1997). Also, the LSTM mechanism is self-learning at some level, adjusting itself to the different patterns exhibited by different individuals, making it less static than its predecessors.

Yet, LSTM models also face demerits due to their relative computational expense and training times as compared to non-sequential approaches such as Random Forests. This could, however, be a factor to consider in applications that are aimed at real-time uses and have limited processing capabilities. However, when it comes to remote work security that requires high levels of accuracy tolerance, LSTM strikes the right point in deploying an accurate yet flexible model combination that enhances secure identity management systems using behavioral biometrics (Keras: Deep Learning for Humans, n.d.).

5. Discussion

It shows a promising possibility that the LSTM networks can take place in enhancing identity verification via behavioral biometrics. With an accuracy rate of nearly 89%, the LSTM model showcases its role in separating legitimate user activity from illegitimate behavior. Comparatively, it's a very good achievement compared to typical machine learning models such as Random Forests and SVM which did not perform quite well as they are unsuitable for sequential data processing. The observations also fall in line with most previous studies that underscore the importance of the LSTM in capturing long-term dependencies in behavioral data(Hochreiter & Schmidhuber, 1997).

This integration has further advanced the growing development of unobtrusive and continuous biometric authentication by keystroke dynamics and mouse movement patterns. Indeed, this raises the emphasis on security in identity verification in remote working environments, as shown in recent literature. Some of these incidents include (Fereidooni et al., 2023), which mention the scalability and robustness of behavioral biometrics using AI to mobile platforms, which make this system suitable for applying it on various devices in different contexts.

Several aspects of AI-based behavioral biometrics have been extensively covered in literature; for instance, continuous group authentication systems aimed at preserving privacy while ensuring security have been advocated for through studies such as that of (Espín López et al., 2023). These aspects seem to be in line with the proposed system focusing on real time monitoring and verification. The study under (Saraswat et al., 2023). advocates the incorporation of anti-spoofing techniques in biometric systems. Incorporating similar protective systems that cater to behavioral patterns may boost overall system reliability. Privacy-preserving designs discussed in work by ("A Privacy-Preserving System Design for Digital Presence Protection," 2023). underscore the need for a secured data handling. This principle is held in this study through encryption and secured data transport. Regulatory challenges that AI imposes on identity verification, according to (Botero Arcila, 2024), are very important insights in aligning the proposed system to its ethical and legal standards. Such studies include that of (Kuric et al., 2024), which show how device-specific differences would influence the accuracy in mouse dynamics. This is also why preprocessing and feature normalization, robust as realized in this study, are essential for the reliability of the system.

Studies connecting AI-driven behavioral biometrics refer to several dimensions, such as continuous group authentication systems which suggest privacy within security, for example, in the study of (Espín López et al., 2023). These comprise monitoring and verification processes in real time about the proposed system.(Saraswat et al., 2023) stressed on the incorporation of anti-spoofing techniques in biometric systems and although this study only concerns behavioral manifestations, using those protective mechanisms may significantly improve system reliability. The work by (A Privacy-Preserving System Design for Digital Presence Protection, 2023) on privacy-preserving designs emphasizes the security handling of data which has been upheld in this study through encryption and secure data transport. (Botero Arcila, 2024) delves into the regulatory challenges brought about by AI with regard to identity verification, which perspectives become of importance to ensure the proposed system in ethical and legal standards. An example would be: The study, for instance, shows that differences specific to a device cause accuracy to vary for mouse dynamics (Kuric et al., 2024). This is vital, because issues are solved by ensuring a sturdy pre-process and feature normalization, as done in the current work for reliability in the system.

Implications of LSTM Neural Networks have on behavioral biometrics are the greatly transformed use of AI in cybersecurity as proving continuous, non-intrusive, and adaptive user authentication, thus enhancing security during remote work-and studies that advocate for the case of optimizing these models for efficiency at the same time accuracy from future perspectives. However, heavy computation involved in such models may not support real-time applications as well in limited-resource settings.

In the recent past, this study has significantly contributed to the continued shoring up of evidence that constitutes a case for the already existing use of AI-powered behavioral biometrics as a consideration for securing identity verification systems in an attempt to allay security concerns clouding the modern digital workspaces.

6. Conclusion

To summarize this discussion meaningfully, the use of LSTM neural networks for behavioral biometrics in identity management systems has a very high promise towards improving the security of staff who work away from their offices. The capability of the LSTM model to analyze sequences of data like keystroke dynamics and mouse movements effectively helps in user behavior models especially in differentiating between normal and abnormal usage patterns even to a very high degree. This approach makes use of the ability of the LSTM network to identify and utilize the long-term dependencies of the data which is an important factor in identifying the subtle characteristics of user behavior over time.

Nonetheless, in an appropriate case, the LSTM can outperform other traditional paradigms, for example, Random Forests or Support Vector Machines, when re-working with serial datasets. This underlines its applicability in situations where there is a need to track and evaluate user behavior around the clock. Indeed, the proposed network is more reservoir consuming, but its capacity to learn different movements for separate users in users' busy lifestyles justifies its employment even in access-controlled environments where identity verification is done remotely. This study highlights the importance and impact of AI-based behavioral biometrics for security, which motivates further research endeavors in enhancing telework and identity verification systems.

References

1. A Privacy-Preserving System Design for Digital Presence Protection. (2023). *Computers, Materials and Continua*, *75*(2), 3091–3110. https://doi.org/10.32604/cmc.2023.032826
2. Bajaj, S., & Kaur, S. (2013). *Typing Speed Analysis of Human for Password Protection (Based On Keystrokes Dynamics)*. https://www.semanticscholar.org/paper/Typing-Speed-Analysis-of-Human-for-Password-(Based-Bajaj-Kaur/b4ee2baeb2c9a58332199850a7c1f795f29c7fde
3. Banerjee, S. P., & Woodard, D. (2012). Biometric Authentication and Identification Using Keystroke Dynamics: A Survey. *Journal of Pattern Recognition Research*, *7*(1), 116–139. https://doi.org/10.13176/11.427

4. Botero Arcila, B. (2024). AI liability in Europe: How does it complement risk regulation and deal with the problem of human oversight? *Computer Law & Security Review*, *54*, 106012. https://doi.org/10.1016/j.clsr.2024.106012
5. *Deeplearningbook*. (n.d.). Retrieved November 19, 2024, from https://www.deeplearningbook.org/contents/mlp.html
6. Espín López, J. M., Huertas Celdrán, A., Esquembre, F., Martínez Pérez, G., & Marín-Blázquez, J. G. (2023). CGAPP: A continuous group authentication privacy-preserving platform for industrial scene. *Journal of Information Security and Applications*, *78*, 103622. https://doi.org/10.1016/j.jisa.2023.103622
7. Fereidooni, H., König, J., Rieger, P., Chilese, M., Gökbakan, B., Finke, M., Dmitrienko, A., & Sadeghi, A.-R. (2023). *AuthentiSense: A Scalable Behavioral Biometrics Authentication Scheme using Few-Shot Learning for Mobile Platforms* (No. arXiv:2302.02740). arXiv. https://doi.org/10.48550/arXiv.2302.02740
8. Hochreiter, S., & Schmidhuber, J. (1997). Long Short-Term Memory. *Neural Computation*, *9*(8), 1735–1780. https://doi.org/10.1162/neco.1997.9.8.1735
9. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804
10. *Keras: Deep Learning for humans*. (n.d.). Retrieved November 19, 2024, from https://keras.io/
11. *Keystroke Dynamics—Benchmark Data Set*. (n.d.). Retrieved November 19, 2024, from https://www.kaggle.com/datasets/carnegiecylab/keystroke-dynamics-benchmark-data-set
12. Kuric, E., Demcak, P., Krajcovic, M., & Nemcek, P. (2024). Is mouse dynamics information credible for user behavior research? An empirical investigation. *Computer Standards & Interfaces*, *90*, 103849. https://doi.org/10.1016/j.csi.2024.103849
13. *Mouse dynamics*. (n.d.). Retrieved December 22, 2024, from https://kaggle.com/code/jaafarnejm/mouse-dynamics
14. Parate, S., Josyula, H. P., & Reddi, L. T. (2023). Digital identity verification: transforming KYC processes in banking through advanced technology and enhanced security measures. *International Research Journal of Modernization in Engineering Technology and Science*, *5*(9), 128-137.
15. Robust Facial Biometric Authentication System Using Pupillary Light Reflex for Liveness Detection of Facial Images. (2023). *CMES - Computer Modeling in Engineering and Sciences*, *139*(1), 725–739. https://doi.org/10.32604/cmes.2023.030640
16. Saraswat, D., Bhattacharya, P., Shah, T., Satani, R., & Tanwar, S. (2023). Anti-spoofing-enabled Contactless Attendance Monitoring System in the COVID-19 Pandemic. *Procedia Computer Science*, *218*, 1506–1515. https://doi.org/10.1016/j.procs.2023.01.129
17. *StandardScaler*. (n.d.). Scikit-Learn. Retrieved November 19, 2024, from https://scikit-learn/stable/modules/generated/sklearn.preprocessing.StandardScaler.html
18. Stragapede, G., Vera-Rodriguez, R., Tolosana, R., Morales, A., Acien, A., & Lan, G. L. (2022). *Mobile Behavioral Biometrics for Passive Authentication* (No. arXiv:2203.07300). arXiv. https://doi.org/10.48550/arXiv.2203.07300
19. Yu, Y., Si, X., Hu, C., & Zhang, J. (2019). A Review of Recurrent Neural Networks: LSTM Cells and Network Architectures. *Neural Computation*, *31*(7), 1235–1270. https://doi.org/10.1162/neco_a_01199