Robust Continuous User Authentication System using Long Short Term Memory Network for Healthcare

Anum Tanveer Kiyani[1], Aboubaker Lasebae[1], Kamran Ali[1], Ahmed Alkhayyat[2], Masood Ur-Rehman4[3], Bushra Haq[4], and Bushra Naeem[4]

[1] Faculty of Science and Technology, Middlesex University London, United Kingdom
[2] E-Learning Department, Islamic University, Najaf, Iraq
[3] James Watt School of Engineering, University of Glasgow, Glasgow, UK
[4] FICT, BUITEMS, Pakistan
AK1933@live.mdx.ac.uk

Abstract. A traditional user authentication method comprises of username, passwords, tokens and PINs to validate the identity of user at initial login. However, a continuous monitoring method is needed for security of critical healthcare systems which can authenticate user on each action performed on system in order to ensure that only legitimate user i.e., genuine patient or medical employee is accessing the data from user account. In this aspect, the perception of employing behavioural patterns of user as biometric credential to incessantly re-verifying the user's identity is being investigated in this research work to make the healthcare database information more secure. The keystroke behavioural biometric data represents the organisation of events in such a manner which resembles a time-series data, therefore, recurrent neural network is used to learn the hidden and unique features of users' behaviour saved in time-series. Two different architectures based on per frame classification and integrated per frame-per sequence classification are employed to assess the system performance. The proposed novel integrated model combines the notion of authenticating user on each single action and on each sequence of actions. Therefore, firstly it gives no room to imposter user to perform any illicit activity as it authenticates user on each action and secondly it tends to include the advantage of hidden unique features related to specific user saved in a sequence of actions. Hence, it identifies the abnormal user behaviour more quickly in order to escalate the security especially in healthcare sector to secure the confidential medical data.

Keywords: Continuous Authentication · Periodic Authentication · Keystroke Dynamics · Recurrent Neural Network.

1 Introduction

Computer systems and networks are essential part of almost every aspect of human life. All the businesses, healthcare, banking systems, government services,

medical, aviation, communication, education and entertainment are mainly controlled by computer systems. Each organisation is effectively using computer systems to store important information and data including confidential financial transactions, employee records, personal and business emails and medical history. However, this escalating dependence on computers has excavate new computer security threats as well. Moreover, cybercrimes have also been escalated owing to the presence of imposter users who can masquerade the legitimate user in order to get access to system resources which can result into serious exploitation and obliteration of personal, governmental and medical information. In order to preclude the imposters to steal those confidential information and files, one important factor is robust continuous user authentication (CUA) system which can validate the users' identity on each action while accessing the medical records.

The behavioural biometrics i.e., keystroke dynamics can collect the regular behavioural data about the user while interacting with system or relevant device. Hence, this type of behavioural biometric data highly depends on the specification of hardware device or background context [7].

The scholarly works, presented in literature review in domain of CUA using behavioural biometrics, mostly rely on statistical features based on mean and standard deviation of those features [2]. These approaches had considered to maintain the static database of the relevant extracted features. However, this approach has few shortcomings: Firstly behavioural biometrics tend to change gradually with time or based on configuration and specification of different hardware devices. Therefore, the main disadvantage of maintaining a static database of users populated with statistical features could affect and decrease the performance or accuracy of system over time. Secondly, behavioural data i.e., keystroke dynamics, represents a sequential events of time-series which can contain hidden information regarding the specific behaviour of user which cannot be represented with statistical feature profiles of users as well as traditional classification methods cannot mine these type of features to distinguish one user from other.

Continuous user authentication (CUA) problem is not new in the research domain, however, the preceding research conducted in this domain [1] had mostly focussed on periodic user authentication (PUA) based on fixed block of actions which can give room to imposter user to perform illicit activities. In contrast, a true CUA mechanism should authenticate the user on each action. However, keystroke sequential series, consisting of more than one action, can contain unique and hidden features related to specific user. For instance, it can be the unique behaviour of specific user to commit mistakes while typing some specific words or it might be regular user behaviour to open files on system by double clicking the mouse button instead of right clicking on file and then press OPEN option. This type of behaviour can be saved in a sequential series. In this regard, we have proposed a novel approach of integrating the CUA based on single action event and PUA based on keystroke actions sequence in order to improve the system performance.

The main contributions of this work are:

- Recurrent Neural Network (RNN) is used to exploit the time-series nature of keystroke behavioural biometric data.
- A two phase methodology is proposed to authenticate user on each action while accessing the confidential medical records.
- A novel architecture based on integrated per frame LSTM and per sequence LSTM is proposed to combine continuous and periodic user authentication.
- Robust recurrent confidence model (R-RCM) is combined with RNN to continuously authenticate user.

The rest of this paper is arranged as follows: Section II addresses the background of CUA using keystroke dynamics. Section III shows a proposed system model for CUA. Section IV presents the results and assessment of system model. Subsequently, Section V discusses the conclusion of this study.

2 Background

Continuous and Periodic user authentication intend to verify the identity of user after the initial login to ensure that only legitimate user is using the system for the whole session. However, PUA validates the user's identity after fixed time intervals or fixed block sizes in contrast to CUA which can authenticate user on each activity or action. The key requirement for both PUA and CUA is that authentication process should not disturb the user while he/she is performing important tasks on system for which behavioural biometrics i.e., keystroke dynamics can be used. This section presents the background study of CUA / PUA systems using keystroke dynamics. The summary of research works performed on CUA / PUA problem with traditional machine learning methods is presented in Table 1 while the detailed results are discussed below.

Table 1. Machine Learning Methods Works for CUA with Keystroke Dynamics

Work	Users	Features	Block	Method	Results
[1]	53	Duration, digraph latency	500	Neural Network	FAR 0.0152% FRR 4.82% EER 2.13%
[2]	30	Statistical features	1000	Decision Trees	FAR 1.1% FRR 28%
[14]	200	Trigraph latency	900 words	Kernel Ridge Regression	EER 1.39%
[4]	34	Digraph latency	14 Digraphs	Support vector machine	EER 0.0 - 2.94%
[9]	20	Hold time, Digraph	6 blocks	One class SVM	FAR = 2.05% FRR=2%
[3]	103	Digraph latency	200	Random forest classifier	EER 7.8%
[10]	150	Digraph latency	—	Ensemble Classifier	FAR 0.10% , FRR 0.22%
[8]	75	Digraph latency	50 actions	CNN, RNN	EER 4.77%

The initial research on CUA / PUA employing keystroke dynamics had been proposed in 1995 with some insistent results[11]. Afterwards, the researchers in [1] presented a notable system model based on neural networks for CUA/PUA using Keystroke dynamics. Subsequently, block size of 500 keystroke actions had been used with digraph features and achieved the FAR= 0.0152%, FRR = 4.82% and EER = 2.13%.

Moreover, in [2] researchers had used Decision trees for the classification of keystroke data with the average block size consisting of 1000 action events and reported the FMR= 1.1% and FNMR= 28%. Another research work in [14] had used the kernel ridge regression a truncated RBF kernel along with block size of 900 words. In this work, trigraph latency features were used and reported results were EER of 1.39%.

Subsequently, support vector machine technique had also been exploited by researchers in [4] with varying digraph sets for implementing CUA and achieved the EER of 0.0- 2.94% with different sets of digraphs. The researchers in [9] had implemented an architecture named Spy Hunter for CUA using KD which utilised two 1-class support vector machines classifiers. They had used a single key hold time and digraph latency to build the feature vector and block size of 6 actions are used to classify a user after each block. The resultant FAR reported was 2.05% and FRR was 2.0% Additionally, random forest classifier had been used in [3] with block size of 200 keystroke actions and the resultant EER as reported was 7.8%.

Moreover, the researchers in [10] had implemented the competitive selection ensemble classifier approach based on Random Forests (RF), Bayes Net (BN) , decision trees , Support Vector Machine (SVM), Random Tree (RT) and RIDOR RIpple-DOwn Rule learner (Ridor). They showed that employing an ensemble approach as compared to stand alone classifiers can improve the accuracy of system because keystroke dynamics being a weak behavioural biometric modality suffers from behavioural invariability issue. They had reported the FAR= 0.10% and FRR = 0.22% with ensemble classifier. Researchers in [8] had employed the deep neural architecture consisting of convolutional neural network (CNN) and Recurrent neural network (RNN) on the free text dataset and achieved EER= 4.77%.

It can be observed that most of the preceding research works had considered block of actions to authenticate user which can provide a security loophole for imposter user to steal confidential data. Secondly, researchers had considered using the statistical features based on mean and standard deviation with static database which can lead to low accuracy over time since the behavioural biometrics depends on external factors such as age, hardware and background context. In contrast, this research work intended to authenticate user on each single activity and used the keystroke data as a time-series to extract the hidden features with the help of recurrent neural networks which can remember and update the user information as compared to state of art classification methods.

3 System Methodology

This section presents the system architecture of proposed CUA and PUA integrated system. For this purpose, the keystroke dataset presented by University of Buffalo [12] has been used which contains 75 users and 3 different laboratory sessions having a time difference of 28 days between each session.

3.1 Keystroke Sequence Sampling

Keystroke data can be considered as chronological organisation of key down time and key up time events which gives an illustration of sequential time series where each event $i \in I$ consists of the following properties:

- $UserId(i)$ – a user that has performed given action / event.
- $SessionId(i)$ – session id of action / event.
- $DownTime(i)$ – an absolute time when any specific key is pressed.
- $UpTime(i)$ – an absolute time when any specific key is released.
- $KeyCode(i)$ – a key code for any specific key which is pressed and released by user.

Formally, each of these events containing $(UserId', SessionId', DownTime, UpTime, KeyCode)$ are assembled into a group of events to make a keystroke sequential time series as follows:

$$Sequence(UserId', SessionId') = \{i | \forall i \in I, s.t. Where$$
$$UserId(i) = UserId',$$
$$SessionId(i) = SessionId',$$
$$DownTime(i) = DownTime,$$
$$UpTime(i) = UpTime,$$
$$KeyCode(i) = KeyCode',$$
$$\}$$

3.2 System Model

Two types of system architectures are formulated for continuously authenticating a user. Both architectures consists of two-Phase methodology framework where recurrent neural network is the first phase while robust recurrent confidence model (R-RCM) as proposed by authors in [6] is the second phase of proposed framework.

A recurrent neural network (RNN) is mostly used for the problems containing time-series data thereby it can be employed for keystroke dynamics data owing to its sequential nature consisting of organised timestamps for each action. Moreover, robust recurrent confidence model (R-RCM) tends to calculate the confidence of users' genuineness on each action and it decides whether the user can continue using the system or should be locked out.

Phase 1: Long Short Term Memory (LSTM) The refined form of RNN named as Long short term memory (LSTM) [13] is used in this work to eliminate the problem of diminishing gradients of basic RNNs. In contrast to basic RNNs, LSTM works on loop structure and contains memory cell thereby can store and modify the previous information on each time-step hence it can update the keystroke behavioural data with time. The cell architecture of LSTM is shown in Fig 1.

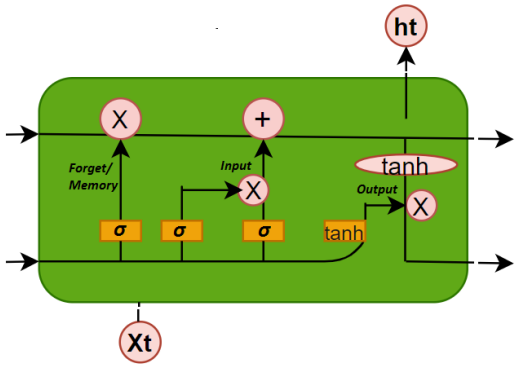

Fig. 1. The LSTM Cell Structure

Phase 2: Robust Recurrent Confidence Model (R-RCM) Robust Recurrent Confidence Model (R-RCM) is the second phase of both proposed architectures. The classification output from LSTM goes into the R-RCM as an input and confidence value increases or decreases based on this input and few other hyper parameters as described in [6]. Two types of thresholds i.e., alert threshold and final threshold are used where if the current confidence of user decreases than alert threshold then RCM works more robustly to identify the imposter user as quickly as possible. Moreover, if the current confidence goes down the final threshold then user is locked out of system.

Architecture 1: LSTM per Frame The architecture of LSTM per frame is illustrated in Fig 2. The raw keystroke data per action/frame is sent into feature extraction unit to generate key monograph and digraph features which afterwards are fed into LSTM unit containing dense layers. The probability of current action is further fed into R-RCM unit to compute the confidence in the genuineness of user and if new calculated confidence is less than the final threshold set by R-RCM, then user would be lock out of system or vice versa.

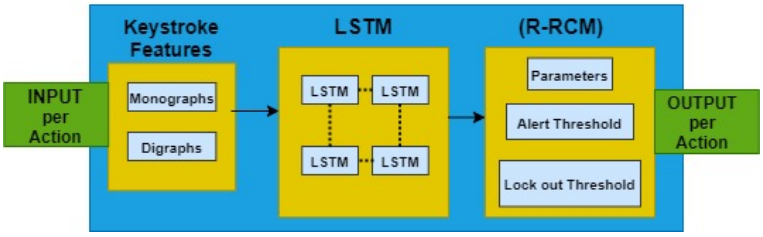

Fig. 2. Architecture 1: LSTM Per Frame

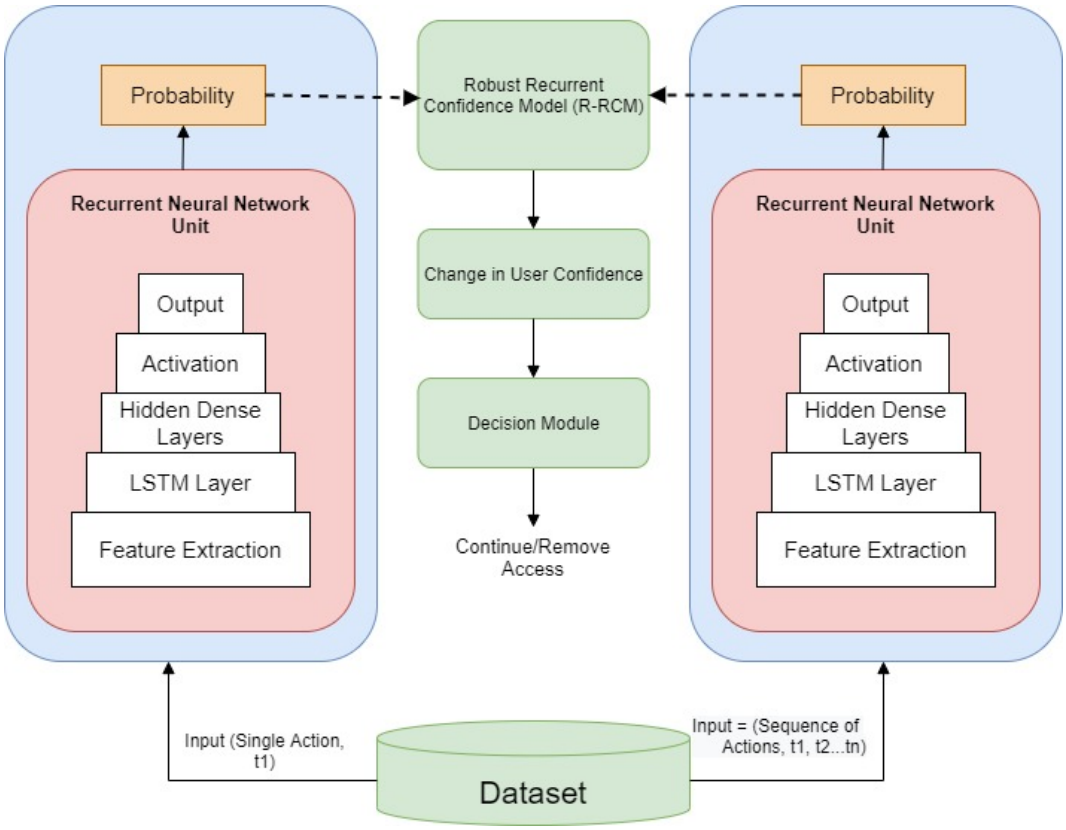

Fig. 3. The System Architecture

Architecture 2: Integrated LSTM per Frame and LSTM per Sequence The proposed architecture integrates the two classification approaches to get the probability based on per action as well as per sequence.

Let's assume, there is a sequence of $M + U$ keystrokes where U is the context length and M is the length of keystroke sequence. Sequences of a defined length $M + U$ have been sampled to generate input features and target user ids with T *time steps* in total.

There are two setups in practice:

- $U = 1$ and $T = M = 1$, a single keystroke action with monograph and digraph features for per frame classification.
- $U = 1$ and $T = M = 64$, a sequence of keystroke actions with monograph, digraph and n-graph features for per sequence classification.

The system architecture has been shown in Fig.3. The first presented model based on per frame classification takes the input data as each action and extracts the action based features containing monographs and digraphs. On the other hand, the second model based on sequence classification segregates the keystroke data into fixed length keystroke sequences and generates the input patterns according to the timing features of keystrokes containing monographs, digraphs and n-graphs. The fixed length sequences used in this study are based on 64 time-steps which contain enough hidden features for the behavioural patterns of given user.

Later on, the prepared sequence comprising the monograph, digraph or n-graph features are fed into the LSTM network which has been efficaciously trained to mine the unique hidden behavioural patterns of user from given sequence. Afterwards, the processed data is sent to fully coupled dense layers and the final probability output is generated.

As shown in Fig 3, the probability output for both models i.e., per frame(left side) and per sequence (right side) goes to the recurrent confidence model (R-RCM) which further processes these inputs along with its hyper parameters to calculate the new confidence level of user. It must be noted that output from per frame LSTM would go into the R-RCM on each action, while the output from per sequence would go into the R-RCM after 64 actions. Therefore, per frame output makes the changes in user's confidence after each action whereas per sequence output makes the change in confidence of user after 64 actions. In a case, when the user's confidence becomes low than the final threshold before the user has completed the 64 actions then the user would be lock out of system without waiting the user to complete the 64 actions sequence.

The core notion of integrating the sequential approach with per frame method is that model can learn the hidden behavioural features from a given sequence and generates an output according to the unique behavioural pattens which cannot be extracted through per frame and also it tends to authenticate the user on each frame hence escalating the system security as well.

Formally speaking, this architecture combines the continuous and periodic authentication owing to classification based on per action and per sequence

strategies respectively. It combines the advantage of per action features which specifies the user behaviour on each action with per sequence features which can depict the unique hidden user behaviour based on general computer usage habits.

4 Results and Discussion

The performance metrics described in [5] for CUA system have been used in this research which are Normalised Average Number of Imposter Actions (ANIA) and Normalised Average Number of Genuine Actions (ANGA).

Suppose there are total U users, each of U cases is allotted two attributes in which first shows if $ANGA = 100\%$ or not, while the second one checks if $ANIA > 40\%$ or not. Based on these two attributes, four user categories are outlined as follows:

- Very Good, $ANGA = 100\%$ and $ANIA \leq 40\%$
- Good, $ANGA < 100\%$ and $ANIA \leq 40\%$
- Bad, $ANGA = 100\%$ and $ANIA > 40\%$
- Ugly, $ANGA < 100\%$ and $ANIA > 40\%$

Fig 4 presents few extracts of the results based on 512 actions, however in practical, testing is done on whole testing set. It shows the results of LSTM per frame architecture where genuine user is tested with its own training sample (left) and it can be observed that genuine user is not falsely locked out by system even once. Similarly, an imposter user is tested with the same genuine user training set (Fig 4 right side), it can be observed that imposter user is locked out by system after performing only few actions marked as L1. After each lockout, it is assumed that imposter user gained access to genuine users' system and its confidence is again set at 1.00. However, on each attempt, imposter user is locked out by system after only performing few actions.

4.1 Aggregated Results of Architecture 1: Per Frame Model

The aggregated results for all the users are presented in tabular form and Fig 5 shows the results in percentages. Table 2 shows the results of stand-alone LSTM per frame model approach. It can be observed that 66 users are falling in very-good category which means these 66 users have never been falsely locked out of system while 9 users are falling in Good category. There are no users in bad and ugly categories. System's ANIA is 0.04 with this approach and ANGA is reported as 0.98.

4.2 Aggregated Results of Architecture 2: Integrated Model

The collective results of Architecture 2 have been listed below in Table 3 and Fig 6 shows the results in percentages. It can be observed that only 3 users have been falsely locked out of system and imposter users have been detected by system after performing only 0.016 portion of actions.

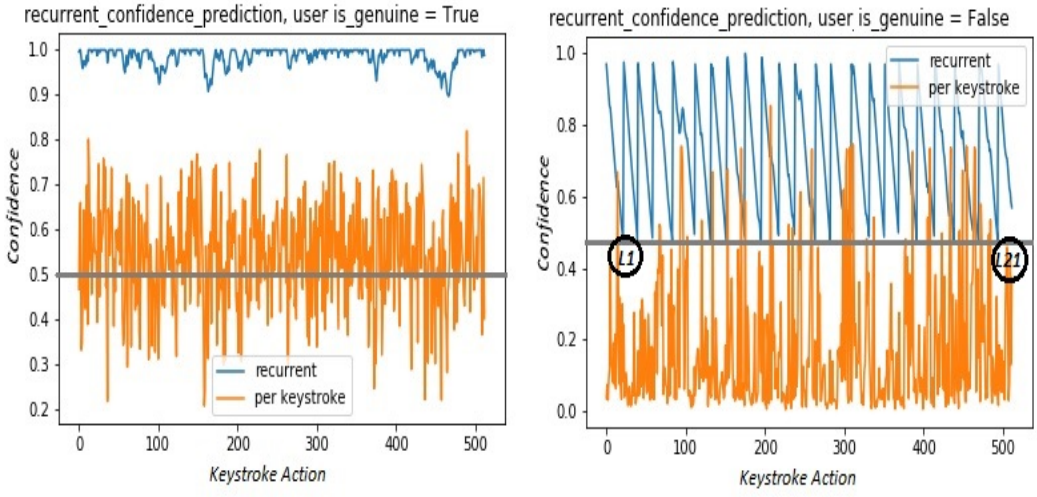

Fig. 4. A Genuine user tested with its own template (left) and with imposter set(right)

Table 2. Architecture 1 (setting III): Aggregated Results of LSTM-Robust RCM

Category	Users	ANGA	ANIA
Very Good	66	1.00	0.04
Good	9	0.88	0.05
Bad	0		
Ugly	0		
System Total	**75**	**0.98**	**0.04**

Table 3. Architecture 2: Aggregated Results of Integrated LSTM per Frame and per Sequence

Category	Users	ANGA	ANIA
Very Good	72	1.00	0.016
Good	3	0.91	0.03
Bad	0		
Ugly	0		
System Total	**75**	**0.99**	**0.016**

4.3 Discussion of Results for Architecture 1 and Architecture 2

If both experimental settings are compared, then it can be observed that architecture 2 has locked out the imposter users on 0.016 % of actions which is quite less than the architecture 1 results(ANIA= 0.04%), hence the imposter users are quickly caught by architecture 2 and also only 3 genuine users are falsely locked out as compared to Architecture 1 where 9 users are falsely locked out

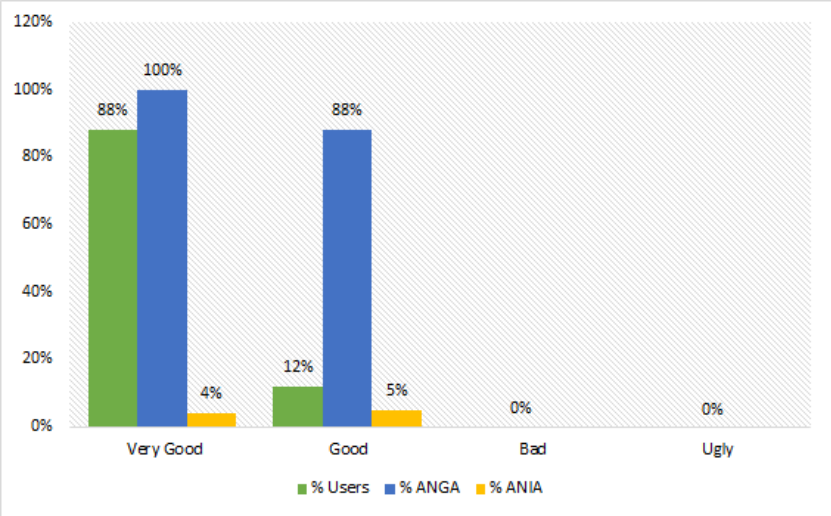

Fig. 5. LSTM- Robust RCM results presented in percentage

by system. System's ANGA and ANIA are improved with architecture 2 which has combine CUA and PUA approaches to continuously authenticate user.

4.4 Results in terms of EER

Equal error rate (EER) has also been calculated to evaluate the results with previous research works. EER is a metric which assesses the data classification performance for any model. In this work, EER has been calculated for both proposed architectures and the results are shown in Table 4 below:

Table 4. Results in terms of EER

Methodology	EER %
LSTM Per Frame	3.2%
LSTM Integrated per Frame-per Sequence	1.04%

If the results of this research work are compared with previous scholarly works given in Table 1, then it can be observed that most of the research works have used the block size of actions and the researchers in [14] achieved the EER of 1.39% but they had utilised the block size of 900 words instead of single keystroke action or sequence size comparative to 64 actions as used in our research to authenticate the user. Moreover, another notable work presented in [8] had also used the RNN for authenticating the users but researchers had used the sliding window approach consisting of sequence of block actions i.e., 50 actions, 100 actions to achieve the EER of 4.77%. In contrast, the results

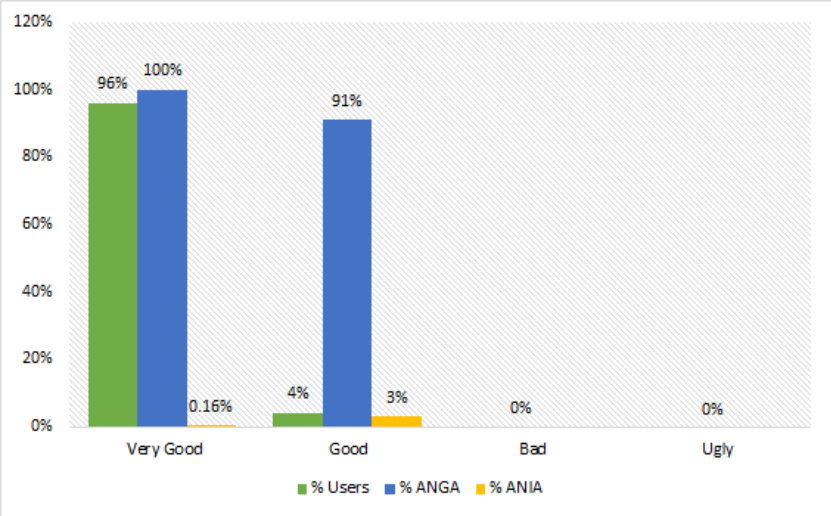

Fig. 6. Integrated LSTM per frame and per sequence results presented in percentage

provided in our research have used the single action(Architecture 1) to achieve 3.2% while we have achieved the lowest error rate (EER) of 1.04% (Architecture 2) precisely with sequence consisting of 64 actions.

5 Conclusion

A robust continuous user authentication model is proposed and implemented which can authenticate user on each action in order to escalate the security of system resources and confidential information in healthcare sector. Since one time validation of user's identity, at the start of session, using usernames and passwords is insufficient to provide optimal security to important medical history and information. In this paper, keystroke dynamics is used as a behavioural biometric modality to continuously authenticate the user on each key press and key release actions while accessing the medical records. In contrast to previous scholarly works, keystroke biometric data is treated as a sequential time-series which can contain hidden unique behaviours patterns of user and these patterns cannot be represented with static database containing mean and standard deviation of features. In this aspect, LSTM model is used which can proficiently learn the time-series data along with the robust recurrent confidence model (R-RCM) that can authenticate user based on each action. Two different architectures based on LSTM per frame and LSTM per Frame-per Sequence are formulated which have considered the behavioural keystroke dynamics data as a set of chronological time-series in order to utilise all the hidden properties of data. The novel proposed integrated architecture, named as per frame-per sequence LSTM model, investigated the effect of combining true continuous user

authentication and periodic user authentication on system performance. It has been observed that proposed integrated model has performed well to identify imposter users in only few actions and also avoided the false lockout of genuine users to a greater extent.

References

1. Ahmed, A.A., Traore, I.: Biometric recognition based on free-text keystroke dynamics. IEEE transactions on cybernetics **44**(4), 458–472 (2013)
2. Alsultan, A., Warwick, K., Wei, H.: Non-conventional keystroke dynamics for user authentication. Pattern Recognition Letters **89**, 53–59 (2017)
3. Ayotte, B., Banavar, M., Hou, D., Schuckers, S.: Fast free-text authentication via instance-based keystroke dynamics. IEEE Transactions on Biometrics, Behavior, and Identity Science **2**(4), 377–387 (2020)
4. Çeker, H., Upadhyaya, S.: User authentication with keystroke dynamics in long-text data. In: 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS). pp. 1–6. IEEE (2016)
5. Kiyani, A.T., Lasebae, A., Ali, K.: Continuous user authentication based on deep neural networks. In: 2020 International Conference on UK-China Emerging Technologies (UCET). pp. 1–4. IEEE (2020)
6. Kiyani, A.T., Lasebae, A., Ali, K., Rehman, M.U., Haq, B.: Continuous user authentication featuring keystroke dynamics based on robust recurrent confidence model and ensemble learning approach. IEEE Access **8**, 156177–156189 (2020)
7. Kiyani, A.T., Lasebae, A., Ali, K., Ur-Rehman, M.: Secure online banking with biometrics. In: 2019 International Conference on Advances in the Emerging Computing Technologies (AECT). pp. 1–6. IEEE (2020)
8. Lu, X., Zhang, S., Hui, P., Lio, P.: Continuous authentication by free-text keystroke based on cnn and rnn. Computers & Security **96**, 101861 (2020)
9. Manandhar, R., Wolf, S., Borowczak, M.: One-class classification to continuously authenticate users based on keystroke timing dynamics. In: 2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA). pp. 1259–1266. IEEE (2019)
10. Porwik, P., Doroz, R., Wesolowski, T.E.: Dynamic keystroke pattern analysis and classifiers with competence for user recognition. Applied Soft Computing **99**, 106902 (2021)
11. Shepherd, S.: Continuous authentication by analysis of keyboard typing characteristics (1995)
12. Sun, Y., Ceker, H., Upadhyaya, S.: Shared keystroke dataset for continuous authentication. In: 2016 IEEE International Workshop on Information Forensics and Security (WIFS). pp. 1–6. IEEE (2016)
13. Tse, K.W., Hung, K.: User behavioral biometrics identification on mobile platform using multimodal fusion of keystroke and swipe dynamics and recurrent neural network. In: 2020 IEEE 10th Symposium on Computer Applications & Industrial Electronics (ISCAIE). pp. 262–267. IEEE (2020)
14. Wu, P.Y., Fang, C.C., Chang, J.M., Kung, S.Y.: Cost-effective kernel ridge regression implementation for keystroke-based active authentication system. IEEE transactions on cybernetics **47**(11), 3916–3927 (2016)