Smart Watch based Body-Temperature Authentication

Timibloudi S Enamamu
Centre for Security, Communications and Network Research, Plymouth University, Plymouth, United Kingdom
timibloudi.enamamu@plymouth.ac.uk

Nathan Clarke
Centre for Security, Communications and Network Research, Plymouth University Plymouth, United Kingdom
N.Clarke@plymouth.ac.uk

Paul Haskell-Dowland
Security Research Institute, Edith Cowan University, Perth, Australia
p.haskelldowland@ecu.edu.au

Fudong Li
School of Computing, University of Portsmouth, Portsmouth, United Kingdom
fudong.li@port.ac.uk

***Abstract*—The advancement of smart devices has led to a steep rise in wearable devices of which smart watches are increasingly gaining popularity in the wearable technology market. Most smart watches have evolved from their first generation to their present generation with increased functionality and capacity. This has led to smart watches gaining popularity and acceptability within the mainstream digital device usage. The first generation of smart watches were fitted with fewer sensors compared to the present day smart watches. The present day smart watch can be used for various activities much more than its tradition usage for health and fitness. These activities includes accepting and declining calls, reading Short Message Service (SMS), listening to music, navigation etc. while smart watches are still advancing technologically, some can function independently while most can be synchronized with smart phones through Bluetooth or Near-Field Communication (NFC). This brings about their easy communication with smart phones. To access the smart watch applications and information, it will be ideal to authenticate the user. Therefore this paper proposed a novel body temperature authentication system, BT-Authen, to authenticate the user by using the body temperature information extracted via a smart watch for continuous and non-intrusive user authentication. The authentication credentials are compared on the smartphone it is paired with before access is granted. To actualise this, the galvanic skins response (GSR) and skin temperature information are extracted for user authentication. The dataset for the evaluation of the body temperature signals are extracted from 30 subjects over three days. Six features are extracted from each of the two body temperature signals. The classification achieved an EER of 3.4 % using a Neural Network Feedforward (NN-FF) classifier. The performance increased to EER of 0.54% after applying a best performance scoring algorithm.**

Keywords*—User Authentication, Smart Phone, Smart watch, Skin Temperature, Galvanic Skin Respond (GSR)

I. INTRODUCTION

Most smart phone manufacturers are venturing into smart watch production with an application to connect them to their smart phones. With the coming of the "internet of things", there has been an increase in their demand in recent years because of their capability and interconnectivity with personal devices [1]. There are more sensors embedded in the current generation of smart watches with improvement on every later version rolled out. This development has seen a rise in third party applications that can connect these smart watches to varieties of smart phones. Their simple connectivity, convenience, and easy usage in place of a regular watch has accelerated their adaption. With smart watches ability to communicate with other smart devices that they are compatible with, it can access and receive information like email alert, text messages, phone calls, Short Message Service (SMS) among others as stated earlier. This is typically carried out via Bluetooth or Near-Field Communications (NFC) paired to the smart phone [2, 3, 4]. After a smart phone is paired with a smart watch to receive information from the phone, it is most likely to remain so until it is unpaired [5]. A smart watch is paired to a phone is for easy access to receive personal information like email alert, text messages, phone calls, Short Message Service (SMS) among others. This information is accessible on the smart watch by anyone as long as the watch have received the information. An unauthorised user can access the applications and information therefore it will be necessary to authenticate the user before access granted to the smart watch.

The aim of this proposal is to authenticate the user of the smart watch on continuous bases before allowing access to the smart watch application and information. The question is, do all smart watches implement a user authentication mechanism? If they do, how strong are the authentication methods? To answer these questions, it is therefore necessary to examine the authentication methods implemented in smart watches. Most

978-1-5090-4642-3/17/$31.00 ©2017 IEEE

smart watch security mechanism have proven to be weak [7, 8] such as the case of the Samsung Gear S3 hack [9]. Fitbit is a popular smart watch producer with many personal health metrics but lacks in user authentication mechanism which makes it vulnerable to attack [10]. Pebble smart watches are also popular but also lacks security mechanisms [4]. The Apple watch, only locks when it is out of the range of the paired phone with an optional prompt for Personal Identification Numbers (PIN) [11]. Most smart watch users go for price-sensitive, generic smart watches which are compatible with most android phones but many have no user authentication mechanism [11]. The size of smart watches and their lack of a keyboard make it difficult to design an authentication mechanism for them [12]. Most users ignore smart watch user authentication because of the small surface area of smart watches makes it difficult to input a security lock. There are other constrains in implementing a user authentication mechanism for smart watches, this includes power consumption, communication capacity, design constraints compared to other smart devices [13].

This work seeks to continuously authenticate the user of the smart watch. The continuous user authentication mechanism is implemented on the phone, allowing information to be transmitted after the presented authentication information is verified. User authentication is implemented as knowledge base, token base or biometric base. Biometric base user authentication stands out as the most appropriate approach for mobile devices which include smart watches [14]. Biometric user authentication uses the biometric sample presented against the sample stored as a template. Body temperature is a viable bioelectrical signal for use in this regard because the smart watch can extract the body temperature [15] while the user is wearing the watch. User authentication on the smart watch is most likely to fail when it is detached from the wrist or when a different person wears it. This has many advantages compared to the use of password, Personal Identification Number (PIN) or pattern pass/phrase.

The proposed method will be unrestrictive and in real time allowing users to go about their daily activities. Most smart watches presently in the market are fitted with sensors that can extract varieties of bioelectrical signals. These bioelectrical signals are not limited to body temperature information like skin temperature and Galvanic Skin Response (GSR) alone. Skin temperature is the body's ability to generate and expel heat while GSR is the electrical conductance of the skin which is associated with the sweat glands [16].

Most prior works on the use of smart watches for authentication considered on their usage for implementing user authentication before a mobile device is accessed. These works includes gait [17, 18], motion-based [19], implicit sensor-based (20), accelerometer based [21], context-aware [22], activity-based implicit [23] and many more. Protecting information on the phone with a user authentication mechanism in place does not stop the information from transmitting to the watch as long as the two devices are paired. To this extent, this work looked at preventing information from the phone to be transmitted to the smart watch without the phone authorising it. The phone authorises only a wearer of the smart watch whose biometric sample have been stored on the phone for user authentication. This is novel as no work has applied this method for protecting information on the smart phone to the best of the author's knowledge.

II. Related work

Recent research has shown body temperature to be promising from the few works relating to the use of body temperature which includes skin temperature and GSR. [24] monitored the skin temperature after immersion of the subjects in cold water intermittently for 1 hour three times a week for 4 to 6 weeks. The experiment shows slight changes in the skin temperature because of the acclimatization of the cold condition mostly on the lower part of the body. There was a little increase noticed in the level of body fat. To support this information, Toner's research on thermal adjustment due to cold water immersion of the body [25] further authenticates the work about the variation of body fat and body temperature difference. It shows that after a period of time the metabolic system stabilizes influence by clothing and body fat in a cold environment [26]. In another work by [27] the skin temperature on different parts of the body including the finger, palm, forearm, thigh, trunk, and forehead from six volunteers with the same physical fitness were measured. The result shows little fluctuation in all the part measured even at standing position to identify a person. The skin temperature on the finger, palms and the forearm have a periodic cycle of amplitude up to 1°C which is an advantage on the use of body temperature measurement to identify a person. In more work on skin temperature, [8] used skin temperature as a second layer for verification of a user's presence after user authentication deploying a wearable device for nomadic application login. In the work, the skin temperature is amplified due to voltage swing to normal skin temperature range before passing it through a low-pass filter to remove sudden changes in temperature. An alarm is built into the system to trigger if the temperature changes rapidly during the login duration which might be as a result of detachment of the

wearable. The skin temperature is used to make a decision on the detachment of the wearable device from the user's body.

The use of GSR is more prevalent compare to skin temperature for human emotional recognition [28, 29, 30, 31, 32]. Kim [28] in his work used four physiological signals which includes skin temperature and skin conductance from a database for signal-based emotion recognition system. The emotion based recognition system used sadness, anger, stress and surprise as the emotion activity data. Eighty subjects were used for the work with the statistical features of mean and maximum value. The features were extracted without any pre-processing from the skin temperature within fifty second intervals. From the skin conductance, the mean of the Direct Current (DC) level, mean of the value of skin conductance response occurrence in the fifty second time frame were used as the features. The best classification results are 61.76% and 78.43% for the stress and surprise. In another work [29], it used the same physiological signals just like Kim to extract 17, 20 and 22 features from a subjects emotion and using canonical correlation analysis for classification with a recognition result of 82%, 85.3%, 85.3% respectively[30].

III. METHODOLOGY

The goal for this work is to use data collected in a natural environment, therefore there was no restriction on when the participants should wear it. The data set is extracted from a smart watch (the Microsoft Band 2) which can extract both GSR and skin temperature. 30 subjects were used with each subject spending a minimum of four hours each day for three days doing regular daily activities. The activities are not defined but each subject was expected to be active cumulatively for at least one hour of the four hours doing their normal daily routines.

A. Experiement

The experiment underlying covered days is to establish the effect of the environment and the change in body temperature over time. The first experiment data set is extracted for 4 hours and divided into 60% for training and 40% for testing. The second set of training carried out with two days data for training and testing. The strategy used two separate sets of data for training and testing. The first day's data is used for training and the second's day data for testing. The last experiment is done with the three days data. The first two days is used for training and the third day date for testing. This is to further predict and understand the day to day variance of the modalities. Other information about the data used is shown in Table 1.

Table 1. Showing the 3 data set information for GSR and Skin Temperature (ST) for the 30 subjects

Data Types	**Day 1**	**Day 2**	**Day 3**
Number of Features Extracted	6 (GSR) and 6 (ST)		
Number of Feature Segments of each Subject	600	1200	1800
Number of days for extraction	1	2	3

B. Pre-processing

The pre-processing of data includes noise removal and reducing the dimensionality of the signal before applying feature extraction [33]. Most signals used for biometric authentication are pre-process by applying a filter to reduce or eliminate the noisy part of the signal. The signal extracted is expected to be noisy therefore filtering of the signal is necessary to avoid aliasing because of the body temperature range [6] however filtering was not directly applied to the signal before extracting the features because filtering is underlined in the use of wavelet for feature extraction [32, 34]. The time frame for continuous authentication is an important aspect because it should contain enough information for verifying the user [35] therefore the data set is segmented into a time frame of three and five seconds for comparison in the first instance. Three seconds is adapted for the final evaluation after a preliminary work using 5 subjects.

C. Feature Extraction

Wavelet transform is a popular tool for pattern recognition and analyzing of non-stationary signals with the ability to represent low frequency effectively into specific time and frequency component [36]. We investigated and apply the most appropriate wavelet feature extraction methods. Wavelet coefficient and wavelet packet extraction methods were chosen [37]. An initial experiment is conducted using five subjects provided an opportunity to examine the data in depth. From the five subjects, 12 statistical features are applied on discreet wavelet transform (DWT) coefficient and 6 entropy features applied to wavelet packet. The statistical features includes mean, maximum amplitude, minimum amplitude, maximum energy, minimum energy, standard deviation, peak to peak, median, root-mean-square (RMS) and peak-magnitude-to-RMS ratio from the wavelet coefficient while the wavelet Packet entropy features are Shannon entropy, energy entropy, threshold entropy, sure entropy and normalised entropy.

Comparing the graphical results, it shows that the features extracted using DWT were not discriminatory enough to differentiate subjects both for the GSR and skin temperature as show in Figures 1 and 2. The statistical features from the GSR have shown only subject 1 was discriminative while the

features had insignificant output across all four subjects. The skin temperature has two; the minimum energy and peak-magnitude-to-RMS features that could discriminate subjects and the remaining features had no output to discriminate the subjects.

In comparison, the wavelet entropy features have given useful information for discriminating the five subjects as seen in Figures 3 and 4. From the graphical interpretation, the skin temperature has shown more discriminatory information than the GSR however fusion of the two modalities may reduce the user authentication equal error rate (EER).

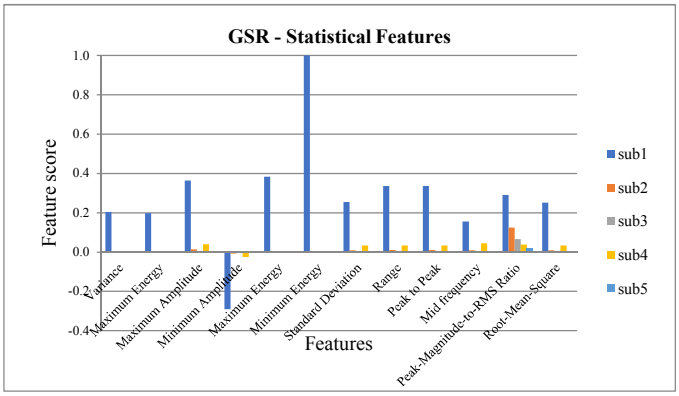

Figure 1. Statistical Feature extracted from GSR

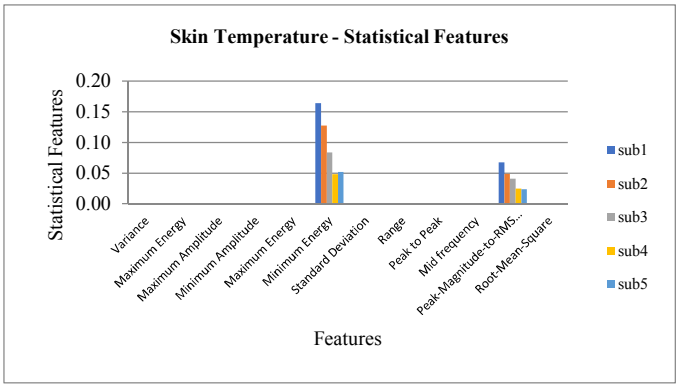

Figure 2. Statistical Feature extracted from Skin Temperature

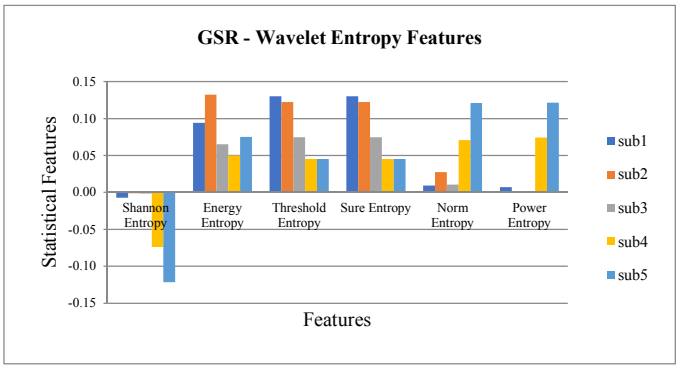

Figure 3. Wavelet Entropy extracted from GSR.

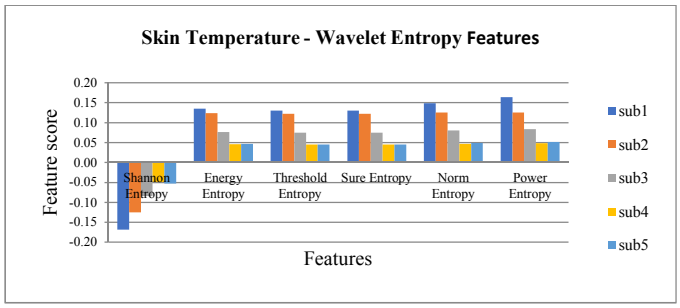

Figure 4. Wavelet Entropy extracted from Skin Temperature

The six features from the wavelet packet entropy has shown its ability to extract most of the signal energy for effective representation which is an advantage of wavelet entropy [38]. Using Matlab (wentropy), the Shannon entropy, energy entropy, threshold entropy, sure entropy, norm entropy and power entropy were computed to extract the features [39].

- **Shannon entropy**: computes the original entropy of the signal.

Shannon entropy = wentropy (signal,'shannon')

- **Energy entropy:** this is the log energy of the signal
  Energy entropy = wentropy (signal, 'log energy')

- **Threshold entropy:** Compute threshold equal to 0.5 entropy of signal
  Threshold entropy = wentropy (signal, 'threshold', 0.5)

- **Sure entropy:** The Sure entropy measures the coefficient of a signal irrespective of the size simultaneously using threshold of 3 [40].
  Sure entropy = wentropy (signal,'sure', 3).

- **Normalized entropy:** Compute norm entropy of the signal with power equal to 1.1.
  Normalised entropy = wentropy (signal, 'norm', 1.1)

- **Power entropy:** Compute power entropy as
  Power entropy = (norm(signal)^2)/length(signal);

D. Classification

The feature output amplitude depends on the body temperature fluctuation therefore to reduce the peak correlation; normalization is applied to the output feature before classification [41]. Different types of classifiers include Support Vector Machine (SVM), k-nearest neighbors (k-NN), Gaussian mixture models and Hidden Markov Models can be used for solving pattern classification problem. This work employed Feedforward Neural Network due to its ability and performance. Neural networks have successfully been used for practical applications in many fields and have shown to be

useful in pattern recognition [42]. The neural network classification learns and behaves like the human brain to recognize patterns and make decision. Neural network is also useful for predicting data base on previously acquired information on the data [33]. Research has also shown that NN-FF works well in conditional estimation [43]. For effectively evaluating the suitability of the features extracted from the body temperature, three different classifications were conducted with data collected for the 1st day, 2nd day and 3rd day. This is conducted to predict the body temperature behaviour and to further forecast the future behaviour because of their instability due to the environmental factor [44]. To predict the intra-day behaviour, the first day data is divided into 60% for training and 40% for testing. It is expected that the same day classification will perform better than inter-day classification. The performance metric used for evaluating the system is the EER. The EER is calculated from the False Acceptance Rate (FAR) and the False Rejection Rate (FRR). The FAR is the acceptance of the system of an impostor while the FRR is the rejection of a legitimate subject by the system.

IV. RESULTS

The results shown in Figure 5 are encouraging with the first day EER at 1.46%. This is a classification of the same day data. The data samples for testing and training are extracted the same day. The 2nd day data achieved a high EER of 2.18%. The data for testing and training are from two separate days. The 3rd day's EER was 3.4% higher than the previous results. The 1st and 2nd day data set was used for training while a 3rd day data was used for the testing. Figure 6 show the performance of individuals of 1st day, 2nd day and 3rd day. The individual result shows the 1st day and 2nd day had a good result of below EER of 5% in most of the user while day 3 had subjects above EER of 10%. In general the EER increased as the days increase.

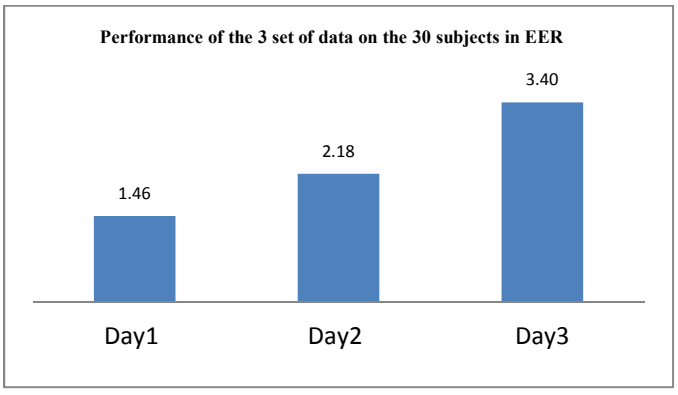

Figure 5. The graphical representation of three results in EER

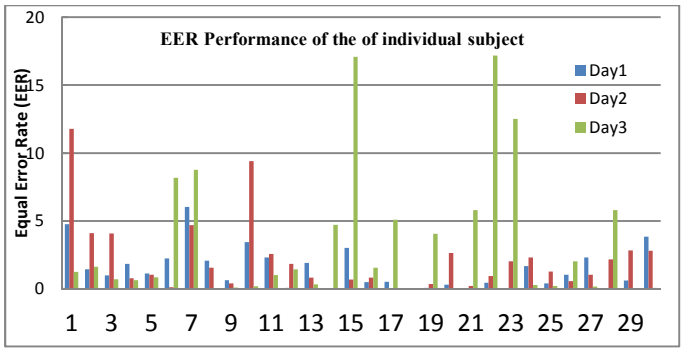

Figure 6.Graphical representation of individual Performance. Day 1 represent data for just one day, Day 2 represent data two days recording and Day 3, three days recording.

V. DISCUSSION

The result shows the intra-day result (1st day) performed better than the rest of the results. This could be attributed to environmental factor [24]. Analysis from the individual EER results shown in Table 2, the 1st day result has 50% of all the subjects achieving EER below 1% but of interest is the fact that the 3rd day has higher percentage (46.6%) of subjects achieving below EER of 1% than the 2nd day with 43.3%. This does not reflect the trend of the result in Figure 5. The 1st day result which had the best performer in EER had total best individual performance at 36.7% which is lower than the 3rd day. Subject 4, 5, 8, 9, 13, 27 and 30 are against the final EER result trend. Their performance is in the reverse, having the best EER on the 3rd day, better result on the 2nd day and the worse result on the 1st day. This indicates the fact that judging from the result analysis, it shows that performance of the system is not mainly affected by day to day environmental temperature factor.

From Table 2 it could be seen that three subjects affected the result of the 3rd day. These Subjects are subject 15, 22 and 23. The EER of the remaining subjects is 1.83%, that mean the three subjects has a combine EER of 1.57% attributed them. It is observed that these three subjects performed well on the 1st day and 2nd day's result. Subject 22 has EER below 1% on the 1st and 2nd day while subject 15 and 23 had EER below 1% on the 2nd and 1st day respectively. The 2nd day's result increase is attributed mainly to subject 1 having an EER of 11.78%. That is scoring 17.4% of the entire EER score on the 2nd day data.

These two sets of subjects show that the body temperature fluctuation was not much judging from individual EER. This is also indicated in the fact that some subjects performed better on 3rd day's data that has the worst combine result. These subjects includes subject 1 (1.25%), subject 3 (0.7%),

subject 4 (0.64%), subject 8 (0.01%), subject 9 (0.09%), subject 10 (0.18%), subject 11 (1%), subject 13 (0.33%), subject 20 (0.01%), subject 24 (0.28), subject 25 (0.22%), subject 27 (0.17%), subject 29 (0.01%) and subject 30 (0.06%). The 3rd day's had 46.6% in term of best individual performance across all the data set.

Table 2: EER of individual subject's performance across all days

EER Performance of Individual Subject of							
Sub.	**1day**	**2days**	**3days**	**Sub.**	**1day**	**2days**	**3days**
1	4.76	11.78	1.25	**16**	0.49	0.82	1.55
2	1.43	4.10	1.63	**17**	0.52	0.00	5.09
3	0.99	4.07	0.70	**18**	0.00	0.00	0.01
4	1.84	0.77	0.64	**19**	0.08	0.36	4.06
5	1.13	1.03	0.84	**20**	0.31	2.64	0.01
6	2.23	0.12	8.17	**21**	0.05	0.21	5.79
7	6.04	4.68	8.76	**22**	0.44	0.95	17.17
8	2.07	1.56	0.01	**23**	0.05	2.03	12.52
9	0.64	0.40	0.09	**24**	1.68	2.32	0.28
10	3.43	9.40	0.18	**25**	0.39	1.27	0.22
11	2.30	2.56	1.00	**26**	1.04	0.57	2.02
12	0.06	1.84	1.44	**27**	2.31	1.04	0.17
13	1.91	0.83	0.33	**28**	0.05	2.16	5.79
14	0.01	0.02	4.71	**29**	0.60	2.82	0.01
15	3.01	0.69	17.07	**30**	3.83	2.81	0.06

From the results presented in this paper, it could be seen in term of individual performance from the best to the worse as the 1st day, 3rd day and 2nd day respectively. The 1st day with 35.7% of all individual performance below 1% could be predicted to perform better because the data is collected the same day. The activities for the day could be identical therefore identical feature are prevalence in the data set. The 3rd day had 33.3 % of all individual performance which is encouraging because it has multiple days of activities more than 2rd day's data with 31%. It should be noted that no specific pattern of activities is required therefore all subjects acted independence of any lay down rule of what to do or not too day. The 3rd day performance shows irrespective of multiple activities across more days the features extracted could discriminate subjects.

To improve on the system, a learning process is introduced for user authentication using best performance scoring algorithm model [37]. The best performance algorithm selects the best EER from the three day's performance in EER. Applying the best score (EER) performance algorithm, the EER result improved from 3.4% to 0.54% as shown in Table 3.

Table 3: The best two average of EER of each subject from day 3.

EER average performance for 2 days data of individual subject									
Sub.	**EER**	**Sub**	**EER**	**Sub.**	**EER**	**Sub**	**EER**	**Sub**	**EER**
1	1.25	**7**	4.68	**13**	0.33	**19**	0.08	**25**	0.22
2	1.43	**8**	0.01	**14**	0.01	**20**	0.01	**26**	0.57
3	0.70	**9**	0.09	**15**	3.01	**21**	0.05	**27**	0.17
4	0.64	**10**	0.18	**16**	0.49	**22**	0.44	**28**	0.05
5	0.84	**11**	1.00	**17**	0.00	**23**	0.05	**29**	0.01
6	0.12	**12**	0.06	**18**	0.00	**24**	0.28	**30**	0.06
Average performance					**0.54**				

VI. Conclusion and Further Work

From the experimental work, the body temperature for smart watch wearer authentication has shown a realistic approach for solving the security issues of transmitting information from the phone to the smart watch without authenticating the wearer. It is expected that over time the weather will have little effect on the system as the human body temperature can easily adapt to the change stabilizing the temperature over a few days. From the experiment it is seen that the fluctuation in body temperature has little or no effect on the system. Where there is temperature fluctuation effect on the system, the best scoring algorithm overcomes the problem. Future work should collect more data from a wider range of subjects and include samples from a longer time period. The scoring will be most accurately examined over more days for a real implementation.

VII. References

[1] D. Evans, "The internet of things - how the next evolution of the internet is changing everything," White Paper. Cisco Internet Business Solutions Group (IBSG), 2011

[2] Nebeling, M., To, A., Guo, A., de Freitas, A. A., Teevan, J., Dow, S. P., & Bigham, J. P. WearWrite: Crowd-assisted writing from smart watches. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 3834-3846) May 2016. ACM

[3] MOBILEIRON 2015 MobileIron Analysis of Smart watch Security Risks to Enterprise Data. *MobileIron,*1.2:https://www.mobileiron.com/sites/default/files/whitepapers/files/smart watch-security-1.2-EN.pdf

[4] Razaque, A., Amsaad, F., Kumar, R., Abdulgader, M., Jagadabi, S. K., & Sheela, S. Pebble Watch security assessment. In *Long Island Systems, Applications and Technology Conference (LISAT),* April *2016 IEEE* (pp. 1-4). IEEE.

[5] Chen, X. A., Grossman, T., Wigdor, D. J., & Fitzmaurice, G. Duet: exploring joint interactions on a smart phone and a smart watch. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 159-168). ACM April 2014.

[6] BISDIKIAN, C. 2001. An overview of the Bluetooth wireless technology. *IEEE Communications magazine,* 39**,** 86-94.

[7] Valizadeh, E. A Survey of Smart watch Platforms from a Developer's Perspective 2015.

[8] Michael C. Wearables security: Do enterprises need a separate WYOD policy? (cited 17 Oct, 2015).[Online] Available:

http://searchsecurity.techtarget.com/answer/Wearables-security-Doenterprises-need-a-separate-WYOD-policy [access date 2/7/2017]

[9] KHAKUREL, J., PÖYSÄ, S. & PORRAS, J. The Use of Wearable Devices in the Workplace-A Systematic Literature Review. International Conference on Smart Objects and Technologies for Social Good, 2016. Springer, 284-294.

[10] CLABURN, T. 2017. Good news: Samsung's Tizen no longer worst code ever. Bad news: It's still pretty awful. *theregister*.

[11] [fitbit. (cited 21 Oct, 2015).[Online] Available: https://www.fitbit.com/my. [access date 20/7/2017]

[12] KHAKUREL, J., PÖYSÄ, S. & PORRAS, J. The Use of Wearable Devices in the Workplace-A Systematic Literature Review. International Conference on Smart Objects and Technologies for Social Good, 2016. Springer, 284-294.

[13] MOBILEIRON, MobileIron Analysis of Smart watch Security Risks to Enterprise Data, 2015. *MobileIron,*1.2:https://www.mobileiron.com/sites/default/files/whitepapers/files/smart watch-security-1.2-EN.pdf

[14] CLARKE, N. L., FURNELL, S. M. & REYNOLDS, P. L. Biometric authentication for mobile devices.

[15] KHAKUREL, J., PÖYSÄ, S. & PORRAS, J. The Use of Wearable Devices in the Workplace-A Systematic Literature Review. International Conference on Smart Objects and Technologies for Social Good, 2016. Springer, 284-294.

[16] Ching, K. W., & Singh, M. M. Wearable technology devices security and privacy vulnerability analysis. *Int. J. Netw. Secur. Appl*, *8*(3), 19-30, 2016.

[17] JOHNSTON, A. H. & WEISS, G. M. Smart watch-based biometric gait recognition. Biometrics Theory, Applications and Systems (BTAS), 2015 IEEE 7th International Conference on, 2015. IEEE, 1-6.

[18] GAFUROV, D., HELKALA, K. & SØNDROL, T. 2006. Biometric Gait Authentication Using Accelerometer Sensor. *JCP,* 1**,** 51-59

[19] YANG, J., LI, Y. & XIE, M. MotionAuth: Motion-based authentication for wrist worn smart devices. Pervasive Computing and Communication Workshops (PerCom Workshops), 2015 IEEE International Conference on, 2015. IEEE, 550-555.

[20] LEE, W.-H., LIU, X., SHEN, Y., JIN, H. & LEE, R. B. 2017. Secure pick up: Implicit authentication when you start using the smartphone. *arXiv preprint arXiv:1708.09366*.

[21] Diep, N.N., Pham, C. and Phuong, T.M., 2015. SigVer3D: Accelerometer Based Verification of 3-D Signatures on Mobile Devices. In *Knowledge and Systems Engineering* (pp. 353-365). Springer, Cham.

[22] Xu, W., Shen, Y., Zhang, Y., Bergmann, N. and Hu, W., 2017, April. Gait-watch: A context-aware authentication system for smart watch based on gait recognition. In *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation* (pp. 59-70). ACM.

[23] Zeng, Y., 2016, April. Ph. D. Forum Abstract: Activity-Based Implicit Authentication for Wearable Devices. In *Information Processing in Sensor Networks (IPSN), 2016 15th ACM/IEEE International Conference on* (pp. 1-2). IEEE.

[24] Jansky, L., Vavra, V., Jansky, P., Kunc, P., Knízkova, I., Jandova, D., & Slovacek, K. Skin temperature changes in humans induced by local peripheral cooling. *Journal of Thermal Biology*, *28*(5), 429-437, 2003.

[25] Lee, J. Y., & Choi, J. W. Influences of clothing types on metabolic, thermal and subjective responses in a cool environment. *Journal of Thermal Biology*, *29*(4), 221-229, 2004.

[26] Lee, J. Y., & Choi, J. W. Influences of clothing types on metabolic, thermal and subjective responses in a cool environment. *Journal of Thermal Biology*, *29*(4), 221-229, 2004.

[27] Jansky, L., Vavra, V., Jansky, P., Kunc, P., Knízkova, I., Jandova, D., & Slovacek, K. Skin temperature changes in humans induced by local peripheral cooling. *Journal of Thermal Biology*, *28*(5), 429-437, 2003.

[28] Li, L., & Chen, J. H. Emotion recognition using physiological signals from multiple subjects. In *Intelligent Information Hiding and Multimedia Signal Processing, 2006. IIH-MSP'06. International Conference on* (pp. 355-358). IEEE. December, 2006.

[29] C. Maaoui and A. Pruski, "Emotion Recognition through Physiological Signals for Human-Machine Communication," in *Cutting Edge Robotics 2010, Vedran Kordic (Ed.)*, 2010.

[30] Cheung, V., & Cannons, K. An introduction to neural networks. Signal & Data Compression Laboratory, Electrical & Computer Engineering University of Manitoba, Winnipeg, Manitoba, Canada. 2002.

[31] GUIDO, R. C. A note on a practical relationship between filter coefficients and scaling and wavelet functions of Discrete Wavelet Transforms. *Applied Mathematics Letters*, *24*(7), 1257-1259. 2011.

[32] Fridman, L., Weber, S., Greenstadt, R., & Kam, M. Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location. *IEEE Systems Journal*, *11*(2), 513-521, 2017.

[33] Bishop, C. M. *Neural networks for pattern recognition*. Oxford university press, 1995.

[34] Li, L., & Chen, J. H. Emotion recognition using physiological signals from multiple subjects. In *Intelligent Information Hiding and Multimedia Signal Processing, 2006. IIH-MSP'06. International Conference on* (pp. 355-358). IEEE, December , 2006.

[35] Ellinas, J. N., Mandadelis, T., Tzortzis, A., & Aslanoglou, L. Image de-noising using wavelets. *TEI of Piraeus Applied Research Review*, *9*(1), 97-109, 2004.

[36] Ellis, R. Entropy, large deviations, and statistical mechanics. Springer, 2007.

[37] Tracy, M. B., Cooke, W. E., Gatlin, C. L., Cazares, L. H., Weaver, D. M., Semmes, O. J., ... & Malyarenko, D. I. Improved signal processing and normalization for biomarker protein detection in broad-mass-range TOF mass spectra from clinical samples. *PROTEOMICS-Clinical Applications*,*5*(7-8), 440-447, 2011.

[38] Varanis, M., & Pederiva, R. Wavelet Packet Energy-Entropy Feature Extraction and Principal Component Analysis for Signal Classification.*Proceeding Series of the Brazilian Society of Computational and Applied Mathematics*, *3*(1), 2015.

[39] Guido, R. C.. A note on a practical relationship between filter coefficients and scaling and wavelet functions of Discrete Wavelet Transforms. *Applied Mathematics Letters*, *24*(7), 1257-1259, 2011

[40] Cristianini, N., & Shawe-Taylor, J.. An introduction to support vector machines and other kernel-based learning methods. Cambridge university press, 2000.

[41] Bishop, C. M. *Neural networks for pattern recognition*. Oxford university press, 1995.

[42] Wooden, K. M., & Walsberg, G. E. Effect of environmental temperature on body temperature and metabolic heat production in a heterothermic rodent, Spermophilus tereticaudus. *Journal of Experimental Biology*, *205*(14), 2099-2105, 2002.

[43] Jacobson, L.. Introduction to artificial neural networks part 2-learning, 2014.

[44] Teoh, A.B. and Ngo, D.C., 2005. Cancellable biometerics featuring with tokenised random number. *Pattern Recognition Letters*, *26*(10), pp.1454-1460.