Hardware Implementation of Dynamics Keystroke Applied for Cloud Computing

Basma M. Hassan, Khaled M. Fouad, Mahmoud F. Hassan

Abstract*— Cloud computing is a growing technology which provides remote access to computing resources and user data. Due to its core philosophy of enabling the user to access his data from anywhere and at any time, cloud computing has a major issue with security and user authentication. Biometric identification is a very good candidate technology, which can facilitate a trusted user authentication with the minimum constraints on the security of the access point. However, most of the biometric identification techniques require special hardware, thus complicate the access point and make it costly. Keystroke recognition is a biometric identification technique which relies on the user behavior while typing on the keyboard. It is more secure and does not need any additional hardware to the access point. This paper presents a hardware implementation of an algorithm based on keystroke dynamics analysis synthesized, simulated and implemented on FPGA. The authentication process is based on the GP methods to test the ability of the distance measure between keystrokes and how to distinguish users through their typing dynamics keystroke.The proposed architecture achieves maximum delay 0.55 ns

***Keywords*—Cloud computing, remote access, biometric identification, access point, Keystroke recognition, FPGA, VHDL.**

I. INTRODUCTION

Nowadays, authentication plays a leading part in data security domains for quality of service and confidence, one of the most technologies which concentrate on authentication process is the cloud computing [1] [2] [3]. Therefore, a data security model using the traditional authentication methods such as passwords tokens or PINs [4] failedto keep up with the challenges presented because they canbe stolen or lost, which means a wake security system. Cloud computing security issues [5] such as access control, authentication and authorization [6] requires a high-guaranteed security model to increase Quality of service and user confidence [7, 8]. Using the internet as the backbone provides resources as a "utility" to end users "as and when needed" basis [9], so how to know that the user who access to his rented part in cloud computing to be the legal user without using a firm authentication technique. Most of the biometric identification techniques [10] require special hardware, thus the complexity of the access point and make it costly. Keystroke dynamics [11] [12] [13] [14] is a biometric identification technique which depends on user behavior while typing on a computer keyboard [15]. It is more secure and does not need any additional hardware to the access point.

Keystroke dynamics is the most apparent sort of biometrics available on computer components, but it has not yet led to real hardware security applications for cloud computing technology, if compared to other biometric techniques. However, we believe keystroke dynamics can be actual tool to help implementing access control systems for computer resources and other related applications like cloud computing Environment. In this paper, the GP method [16] converted to a VHDL(V: Very High Speed Integrated circuit, HDL: Hardware Description Language) [17], then successfully synthesized, simulated and implemented on the Spartan-3E XC3S1600E[18] [19] FPGA (Field Programmable Gate Array) with the programming Xilinx tool ISE Web Pack 9.2i, illustrating that the keystroke dynamics may be implemented such as the others user's biometric techniques (Iris, fingerprints, face, hand geometry, etc.,).

II. RELATEDWORKS

Authorization and Authentication are kind of key security and privacy threats for cloud computing. A lot of research discussed this problem and tried to introduce many solutions and methods to decrease security threats in cloud computing environment. One of the new and most interested researches about keystroke dynamics authentication in cloud computing using mobile presented by Babaeizadeh, Bakhtiari and Maarof [20].This paper proposed strong method of authentication in the password authentication method by combining it with keystroke authentication system that could worked at 97.014% correctlyin authenticating mobile's users to access cloud computing. There is a lot of research also tried to make a hardware implementation of many biometric identification systems on FPGA or DSP such as the following. In [21] proposed an implementation of an algorithm characterization and correlation of templates created for biometric authentication based on iris texture analysis programmed on FPGA. The authentication based on processes like characterization methods based on frequency analysis of the sample and achieved high accuracy of 96.52% and time of16.11 ms.Wakil,Tariq,Humayunand Abbas [22] presented FPGA based architecture for fingerprint recognition by using Xilinx System Generator which can befurther implemented on all Xilinx FPGA gave high accuracy and can be used for high security issues.Gayathri and Sridhar [23] proposed and improved fast thinning algorithmfor Fingerprint Image implemented in MATLAB and simulation results of Xilinx ISE and Modelsim. Based on two modules binarization module and thinning module their Experimental results showed that the algorithm is more efficient than the referred algorithm systems.In [24],Fatt,Tay and Mokpresented a Digital

Revised Version Manuscript Received on August 21, 2015.

Eng. Basma M. Hassan, Department of Electrical Engineering Technology, Faculty of Engineering, Benha University, Benha, Egypt.

Dr. Khaled M.Fouad, Department of Computer Science, Faculty of Computers and Informatics, Benha University, Benha, Egypt.

Prof. Mahmoud F. Hassan, Department of Basic Sciences, Faculty of Engineering, Benha University, Benha, Egypt.

Signal Processor (DSP) implementation of the iris verification algorithm.Using hamming distance method to extract the iris features based on texture analysis. Experiment results showed that the approach has achieved high accuracy of 98.62% and time of198.96ms.Kannavara and Bourbakis[25] have presented a local-global (LG) graph methodology for iris based biometric authentication. The global graph of the presented test image is compared with the global graph of the stored reference image and achieved high accuracy of 92 % and time of0.0149ms. Poinsot, Yang and Brost [26] proposed a biometric system combines two modalities: palm print and face. Hardware implementation of the Texas Instrument Digital Signal Processor and Xilinx FPGA platforms using Hamming distance algorithm, and score fusion then have execution time 0.4 ms.In [27], Liu, Sanchez, Lindoso and Hurtado proposed a hardware implementation based on FPGA for an iris biometric processor. By this solution a reduction of the processing time is obtained and security levels of the whole system are increased due to the reduction of software involved and achieved high accuracy of 88 % and time of2.725 ms. Ryan, Bradley, Randy, Robert, and Neil [28] provided novel hardware implementations which enabled us to discover that three key portions of an iris recognition algorithm can be parallelized. The main result is that the implementation on a modest sized FPGA is approximately 9.6, 324, and 19 times faster than a state-of the-art and achieved time of0.002 ms.Vijayalami and Obulesu [29] presented a generic, flexible parallel architecture, which is suitable for all ranges of object detection applications and image sizes. The architecture implemented the AdaBoost-based detection algorithm, which is one of the most efficient object detection algorithms and achieved minimum period 15.30 ns.In [30], Zhao and Xiedescribed an embed iris recognition system for the personal identification they used only one DSP core which can complete image acquisition, image processing, and communication with the peripheral circuits. The model system not only reduced costs, shorten the development cycle. It provided a good running platform for the high-speed image processing achieved time of 471.56 ms.Vatsa, Singh and Noore [31], presented an accurate non-ideal iris segmentation using the modified Mumford-Shah functional. Depending on the type of abnormalities likely to be encountered during image capture, a set of global image enhancement algorithms is concurrently applied to the iris image. While this enhances the low quality regions, it also added undesirable artifacts in the original high quality regions of the iris image achieved accuracy of 97.21% and 1.82 ms.In [32], Hu and Xieshowed a study of Iris Identification techniques in Authentication. Most modern iris recognition systems are currently deployed on traditional sequential digital systems, such as simple DSPs and data matched one by one, which wasted much time. In their study, iris matching, a repeatedly executed portion of a modern iris recognition algorithm parallelized on an FPGA system demonstrated a 22 times speedup of the parallelized algorithm on the FPGA system when compared to simple DSPs and got out 32 us.Guru Nanak Institute of Technology Student [33] proposed a hardware implementation of iris matching. They presented a parallel processing alternative using Spartan-3AN field-programmable gate arrays (FPGAs), achieving significant reduction in execution time when compared to conventional software based applications. The Hamming distance is employed for classification of iris templates, and two templates were found to match if the hamming distance between them is less than the threshold value.

III. PROPOSED ALGORITHM

The proposed system consists of three stages. The enrollment, the test and the authentication process, each stage satisfied a part of the authentication equation “(9),” to test the ability of the distance measure described in the GP method to distinguish users through their typing dynamics keystroke.

(i) The enrollment phase: the user registration stage consists of many block diagrams such as fig.1 shows.

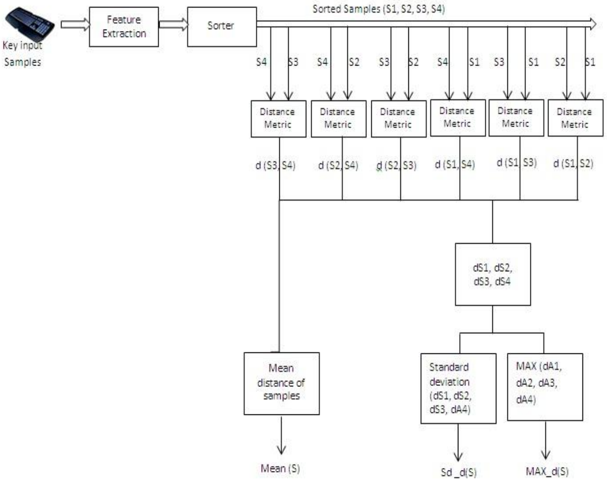


Fig.1.The Enrollment Process

A. *Key input devices*

The sensor of the keystroke authentication system is the keyboard. Individuals can easily run the web page site (JSfiddle) [33] on their own PCs or Laptops. Users are allowed to enter their own dynamic keystrokes containing uppercase characters, lowercase characters, numbers and also special characters.

B. *Feature Extraction*

Features are extracted when users pressed and released keys. There are many algorithms used to find the keystroke features such as the digraph durations (The elapsed time between the depression of the first and of the second key of a digraph). So the feature extraction outputs each digraph the users typed and its duration in milliseconds.

C. *Sorter*

Java Script code which used in the web page created to capture and calculate the user's digraphs duration times then sort the output obtained from the feature extraction block using the Java Script code and output the sorted digraphs ascending according to its duration time as the flow chart in Fig. 2 illustrates.

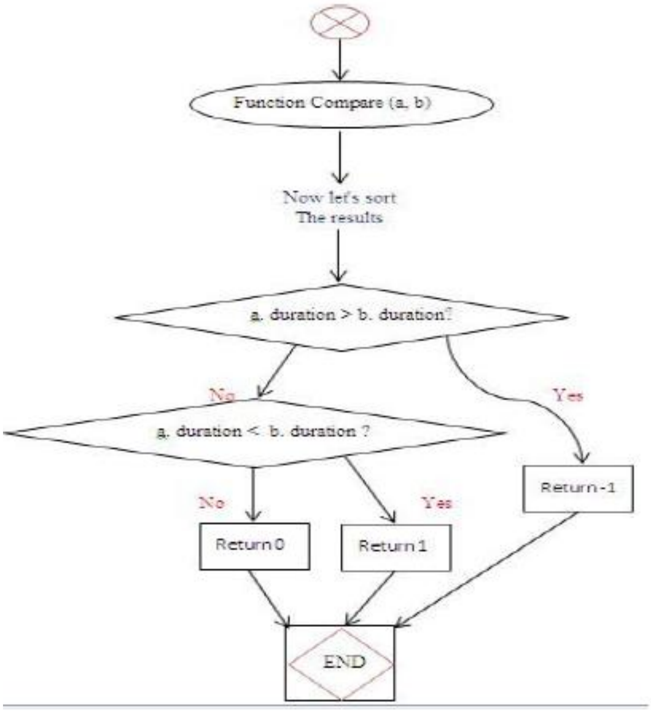
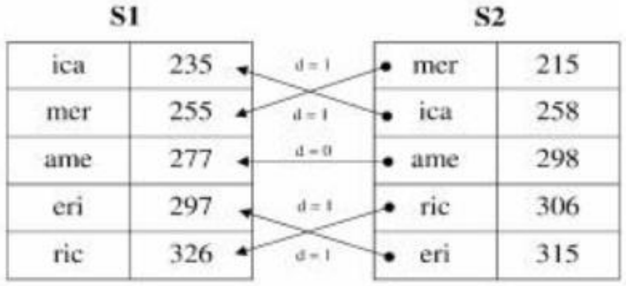


Fig.2. Flowchart to sort digraphs

D. *Distance Metric*

Find the shared element between the two samples to measure of the distance between them [16], and then compute the sum of the distances between the position of each element in S1 and the position of the same element in S2 then divided by

$\frac{N^2}{2}$ If N is even; $\frac{(N-1)^2}{2}$If N is odd where N is the shared element between the two samples as the GP method calculations and illustrates in fig.3.



S1		S2	
ica	235	mer	215
mer	255	ica	258
ame	277	ame	298
eri	297	ric	306
ric	326	eri	315

d = 1
d = 1
d = 0
d = 1
d = 1

Fig.3. Distance Calculation of two typing samples of the same text [16].

User asked to type four samples (S1, S2, S3 and S4). The mean of the distances from samples captured of user A (denoted by m(S)) is: d(S1, S2), d(S1, S3), d(S1, S4), d(S2, S3), d(S2, S4), d(S3, S4). Let mSxyz be the mean distance of samples x, y and z of user A. As an example, mS123 is: mS123 = [d (S1, S2) + d (S1, S3)
+ d (S2, S3)]/3 (1)

For each of the four samples, compute the mean distance of that sample with respect to the other samples of A:

$dS1=|[d(S1,S2)+d(S1,S3)+d(S1,S4)]/3-mS234|$ (2)

$dS2=|[d(S2,S1)+d(S2,S3)+d(S2,S4)]/3-mS134|$ (3)

$dS3=|[d(S3,S1)+d(S3,S2)+d(S3,S4)]/3-mS124|$ (4)

$dS4=|[d(S4,S1)+d(S4,S2)+d(S4,S3)]/3-mS123|$ (5)

E. *Meandistancebetweensamples*

Find m(S) as the following calculation shows to find the mean distances between the user A input samples. m(s) = [d(S1,S2)+d(S1,S3)+d(S1,S4)+d(S2,S4)+d(S3,S4)]/6 (6)

F. *MAX_d (S)*

Find maximum value of the distances from samples (S1, S2, S3 and S4) captured of user A: as the flowchart illustrates in fig. 4.

MAX_d (S) = MAX (dS1, dS2, dS3, dS4) (7)

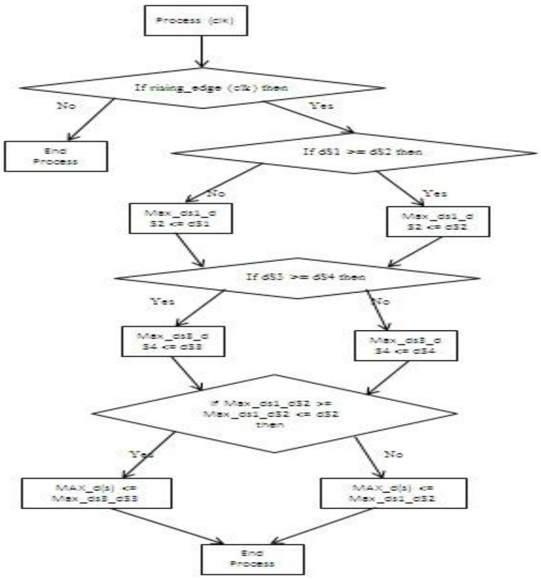


Fig.4. Flowchart to find MAX_d(S)

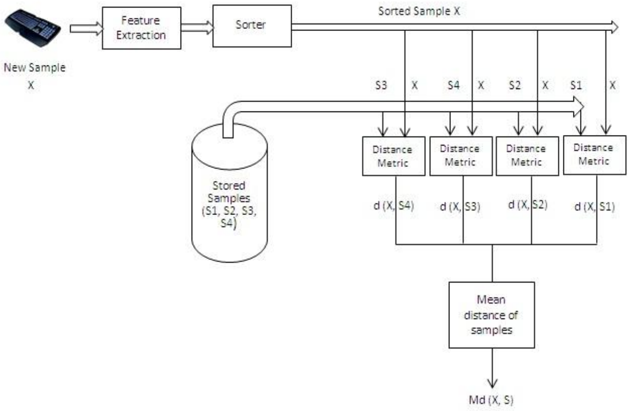
G. *Standarddeviation*

Find the standard deviation which obtained from the previous section: Calculate sd_d(S) = standard deviation (dS1, dS2, dS3, dS4).

(ii) The test stage: The user types a new sample X in web page (JSfiddle) to capture the digraphs duration, then sorted using the sorter, then find the distances between samples (S1, S2, S3, S4) which stored in the database and the new sample X to get:

d (X, S1), d (X, S2), d (X, S3), d (X, S4), then find Md(X, S) as fig.5 illustrates:

Md(X,S)=[d(X,S1)+d(X,S2)+d(X,S3)+d(X,S4)]/4 (8)



5. The verification process

(iii) The authentication process: Accept the user which typed the sample X to be the same user who typed the four samples before and had already stored profile in the database if and only if equation (3) satisfied as the GP method illustrated in his experiment and dissipates in fig.6 where a and b are two constants that should be chosen in order to have an acceptable balance between IPR and FAR.

$$Md\ (X,S) < m\ (S) + a * MAX\_d\ (S) + b * Sd\_d\ (S) \qquad (9)$$

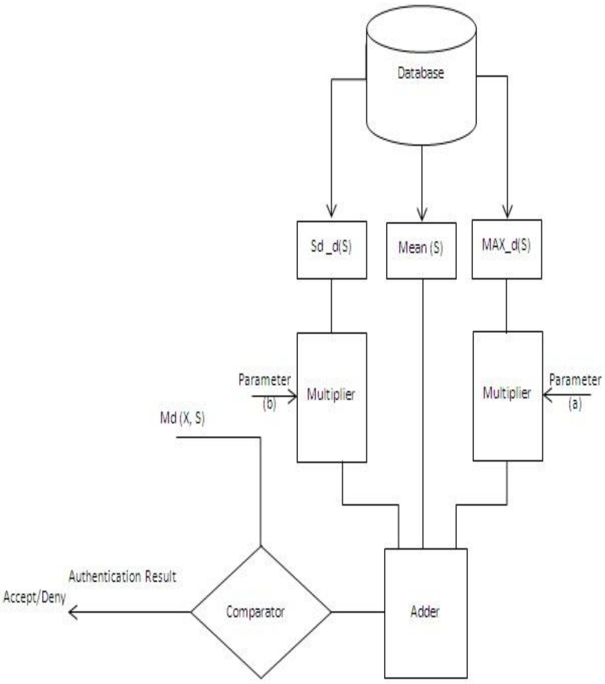
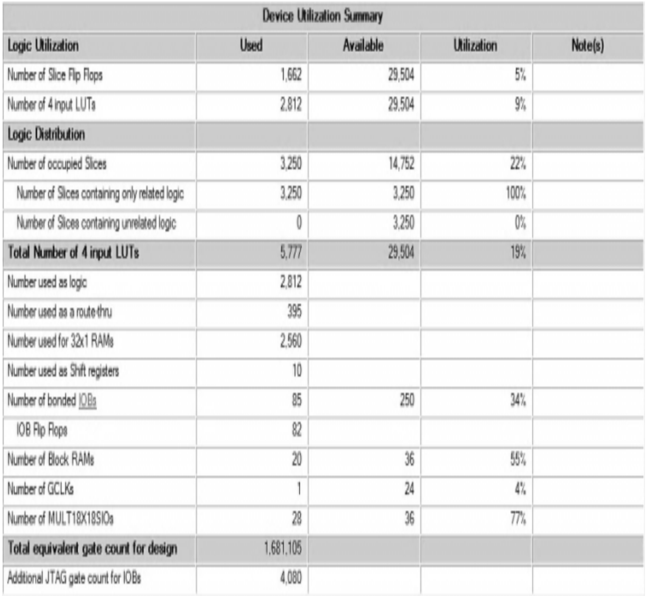


Fig.6.The authentication process

IV. EXPERIMENTRESULTS

Fig.7 shows that there isn't any over-mapping for any of the resources used in the FPGA, allowing the implementation of the hardware architecture of keystroke dynamics in the chosen FPGA device. Memory blocks of dual RAMs (used 20 of the 36 available) and MULT 18*18SIOs (employee 28 of the 36 available) and number of Slices for programmed hardware architecture uses 9% of the available FPGA slices, showing that the hardware implementation of keystroke dynamics has significant resource consumption due to the number of operations that have to be performed. The Spartan-3E FPGA XC3S1600EXilinx is on the Micro Blaze [18][19] Development Kit, this development board has an external memory RAM: DDR SDRAM with 64 MByte, 50 MHz and 66 MHz clock oscillators, ports: HDMI, 10/100 Ethernet PHY, On-board USB-based FPGA, serial, expansion, Four slide switches, Eight discrete LEDs and Four push-button switches, etc. [18]. Figure 9 shows the development board kit which used to implement the proposed system. Comparison between the hardware implementation described in this research and other existing hardware implementations for the other biometric authentication methods will be detailed in table 1. The reviewed method showed different biometric authentication techniques such as face, iris and palmprint. Many articles dissipated minimum execution time like [22], [25], [26], [27] and [28] than the proposed method in this paper, but the point is that the biometric authentication technique used is the dynamics keystroke which is not implemented before in hardware, so the research results illustrates that it can be worked in hardware with acceptable execution time besides the other advantages of this technique also there is a lot of other software programs, but the new here is hardware implementation of dynamics keystrokes.



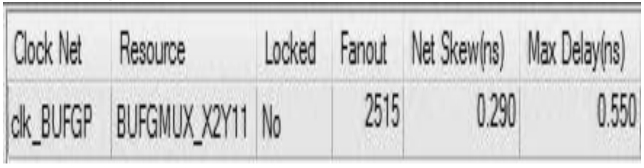
Device Utilization Summary				
Logic Utilization	**Used**	**Available**	**Utilization**	**Note(s)**
Number of Slice Flip Flops	1,662	29,504	5%	
Number of 4 input LUTs	2,812	29,504	9%	
Logic Distribution				
Number of occupied Slices	3,250	14,752	22%	
Number of Slices containing only related logic	3,250	3,250	100%	
Number of Slices containing unrelated logic	0	3,250	0%	
Total Number of 4 input LUTs	5,777	29,504	19%	
Number used as logic	2,812			
Number used as a route-thru	395			
Number used for 32x1 RAMs	2,560			
Number used as Shift registers	10			
Number of bonded IOBs	85	250	34%	
IOB Flip Flops	82			
Number of Block RAMs	20	36	55%	
Number of GCLKs	1	24	4%	
Number of MULT18X18SIOs	28	36	77%	
Total equivalent gate count for design	1,681,105			
Additional JTAG gate count for IOBs	4,080			

Fig.7. FPGA Design Summary

The design should be looking at following two factors for actual FPGA area utilization. - Total no. of occupied slices. (This is 22% in this experiment case) - Total no. of 4-input LUTs. (This is 19% in this experiment case) Each slice has two LUTs and two flip-flops. By looking at the area report the design is more of combinational logic than sequential logic, Because FFs utilization is 5% whereas LUTs utilization is 9%.

A. Clock Report

The results indicate that Max delay which specifies the maximum delay between the clock edges arrives at the FPGA pin and when the synchronous output pin becomes valid is to be (0.550 ns). If you take a signal, and examine the delays to the first and last load: subtract the Slowest (largest) delay from the fastest (smallest) this will give the skew on the signal between the first load, and the last load in this experiment Net Skew is (0.290 ns). All those results show in fig.8.



Clock Net	Resource	Locked	Fanout	Net Skew(ns)	Max Delay(ns)
clk_BUFGP	BUFGMUX_X2Y11	No	2515	0.290	0.550

Fig.8. Clock report results

Table 1: Comparison between the hardware implementation described in this paper and some existing hardware

Reviewed Article	Hardware	Algorithm	Biometric authentication Technique	Time (ms)
Proposed Method	FPGA(Spartan -3e XC3S1600E 1600) CLK: 10MHz	GP method	Dynamics keystroke	49.535 ns
[22]	FPGA(Virtex 5,LX50T) CLK: 100MHz	Frequency correlation using FFT	Iris	16.11
[24]	ADSP-BF561 EZ-KIT LITE CLK: 600MHz	Hamming Distance	Iris	198.96
[25]	FPGA(Virtex 5,xc5vlx30) CLK: 550 MHz	Euclidian Distance	Iris	0.0149
[26]	FPGA Virtex-5 CLK: 175 MHz	Hamming distance and score fusion.	Palmprint and face	0.4
[27]	FPGA(Virtex 4, sx family) CLK: 153.53 MHz	Hamming Distance	Iris	2.725
[28]	FPGA(Stratix IV) CLK: 500 MHz	Hamming Distance	Iris	0.002
[29]	FPGA (Spartan-3E) CLK: 65.432MHz	AdaBoost	Face	15.304 ns
[30]	DSP (TMS320DM642) CLK: 720MHZ	- -	Iris	471.56
[31]	CPU, Pentium IV CLK: 3.2 GHz	Hamming Distance	Iris	1.82

V. CONCLUSIONS

Authentication in cloud computing requires a systemic view, because the security will be constructed along a faraway. Authentication is a very important issue that refers to determine if the individual is the legal person who access to his rented portion. This research suggests the keystroke dynamics as a biometric authentication technique applied to cloud computing technology. A hardware implementation proposed using the GP method for measuring the distance between the user profiles and each new enterto cloud computing.The proposed structure synthesized, simulated and implemented in the Xilinx Spartan-3E FPGA using VHDL code with Xilinx tool ISE Web Pack 9.2i, the best case achievable is 49.535 ns.This research proofs that keystroke dynamics as a biometrics algorithms can be implemented in hardware. The algorithm calculation optimized in order to reduce and overcomes the problem of floating point number. It demonstrates that the operations can be performed with integer numbers without any significant changes in the obtained details.

REFERENCES

1. N. Antonopoulos, and L. Gillam, “Cloud Computing Principles,” Systems and Applications springer -Verlag London Limited, 2010
2. K. Jeffery, B. Neidecker,"the future of cloud computing, "Expert Group Report Public Version 1.0, opportunities for European cloud computing beyond, 2010
3. Cloud Standards Customer Council: Practical Guide to Cloud Computing, Version 2.0, 2014
4. S. Teh, A. Teoh, and S. Yue," A survey of Keystroke Dynamics Biometrics," Hindawi Publishing Corporation, The Scientific World Journal, Volume Article ID 408280, 24 (2013)
5. V.Paranjape andV.Pandey,"An Improved Authentication Technique with OTP in Cloud Computing," International Journal of Scientific Research in Computer Science and Engineering, Vol-1, Issue-3, 2013
6. Emam,"Additional Authentication and Authorization using Registered Email-ID for Cloud Computing,"International Journal of Soft Computing and Engineering ISSN: 2231-2307, Volume-3, Issue-2 (2013)
7. H. Chang and E. ChoiKim," User Authentication in Cloud Computing," UCMA Part II, CCIS 151, pp. 338–342. , 2011
8. M. Kim,H. Jeong, and E. Choi," Context-aware Platform for User Authentication in Cloud Database Computing," International Conference on Future Information Technology and Management Science & Engineering, Vol.14, pp. 170-176, 2012
9. Cloud Computing,(2006), Seminar Report and PPT, available at http://www.seminarsonly.com/computer%20science/Cloud Computing.php
10. A. Babich," Biometric Authentication," Types of biometric identifiers Bachelor’s Thesis Degree Programme in Business Information Technology , 2012
11. S. Rupinder and R. Narinder," comparison of various biometric methods,"international Journal of Advances in Science and Technology (IJAST), ISSN 2348-5426.Vol 2 Issue I, March 2014
12. Monrose,and D. Rubin, "Keystroke Dynamics as a Biometric for Authentication," Preprint submitted to Elsevier Preprint,1999
13. A., Messerman, Mustafic, T., Camtepe, S., and Albayrak, S.: Continuous and non-intrusive identity verification in real time environments based on free-text keystroke dynamics, Int’l Joint Conf. on Biometrics (IJCB), 2011
14. Peacock, X. K, and M. Wilkerson," Typing patterns: A key to user identification," IEEE Security and Privacy, 2(5):40–47, 2004
15. M. Kaur, and R. Virk, “Security System Based on User AuthenticationUsing Keystroke Dynamics,”International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 5, May 2013, pp 2111
16. Bergadano,D. Gunetti and C. Picardi," User authentication through keystroke dynamics," ACM Transactions on Information and System Security (TISSEC) Volume 5 Issue 4, Pages 367-397, 2002
17. P. Ashenden,"the VHDL cookbook the first addition.
18. Xilinx: Spartan-3 Generation Configuration User Guide. Extended Spartan-3A, Spartan-3E, and Spartan-3 FPGA Families UG332 (v1.7) January 27, 2015
19. MicroBlaze Development Kit Spartan-3E 1600E Edition User Guide. December 5, 2007
20. M. Babaeizadeh, M. Bakhtiari and M. Maarof, "Keystroke Dynamic Authentication in Mobile Cloud Computing,"International Journal of Computer Applications (0975 – 8887) Volume 90 – No 1, March 2014
21. S. Prabhakar, S. Pankantiand K. Jain," Biometric Recognition," Security and Privacy Concerns, IEEE Security and Privacy Magazine, Vol. 1, No. 2, pp. 33-42, 2003
22. Giacometto, M. Vilardy, C. O. Torres, and L.Mattos,"Template characterization and correlation algorithm created from segmentation for the iris biometric authentication based on analysis of textures implemented on a

FPGA,"IOP Publishing Journal of Physics, 2011

23. Y. Wakil, S. Gul Tariq, A. Humayun, and N.Abbas, "An FPGA based Minutiae Extraction System for Fingerprint Recognition,"International Journal of Computer Applications (0975 – 8887),Volume 111 – No 12, February 2015
24. S. Gayathri, Dr. V. Sridhar," An Improved Fast Thinning Algorithm for Fingerprint Image,"International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 1, January 2013
25. R. Fatt, Y. Tay, and K. Mok,"Iris Verification Algorithm Based on Texture Analysis and its Implementation on DSP," Int. Conf. on Signal Acquisition and Processing DSP ISBN: 978-0-7695-3594-4, 2009
26. R. Kannavaraand N. Bourbakis,"Iris Biometric Authentication based on Local Global Graphs, An FPGA Implementation," IEEE Proc. Symp. On Computational Intelligence for Security and Defense Applications ISBN: 978-1-4244-3763-4,2009
27. Poinsot, Y. Fan and V. Brost," Palmprint and face score level fusion: hardware implementation of a contactless small sample biometric system," HAL Id: hal-00640727, available: https://hal.archives-ouvertes.fr/hal-00640727 Submitted on 14 Nov 2011
28. J. Liu, R. Sanchez, A. Lindosoand O. Hurtado, "FPGA Implementation for an Iris Biometric," Processor IEEE Int. Conf. on Field Programmable Technology ISBN: 0-7803-9729-0, 2006
29. R. Rakvic, B. Ulis, R. Broussard, and R. Ives, "Parallelizing Iris Recognition," IEEE Trans. On Information Forensics and Security vol. 4 no. 4 ISCN: 1556-6013, 2009
30. Vijayalami, B.Obulesu, "Hardware Implementation of Face Detection Using ADABOOSTAlgorithm,"journal of Electronics and Communication Engineering (IOSRJECE) ISSN: 2278-2834 Volume 1, Issue 2, May-June 2012.
31. Zhao, X. , and Xie, M.: A Practical Design of Iris Recognition System Based on DSP Int. Conf. on Intelligent Human-Machine Systems and Cybernetics ISBN: 978-0-7695-3752-8 , 2009
32. M. Vatsa, R. SinghandA. Noore," Improving Iris Recognition Performance Using Segmentation," Quality Enhancement, Match Score Fusion, and Indexing IEEE Trans, On Systems, Man, and Cybernetics Part B: Cybernetics Vol. 38 NO. 4 ISCN: 1083-4419, 2009
33. Z. Hu, and M. Xie," Iris Biometric Processor Enhanced Module," FPGA-based Design Proc, Second International Conference on Computer Modeling and Simulation 259-62 , 2010
34. http://jsfiddle.net/qLap9/355/Created by the paper group

AUTHOR PROFILE

Eng. Basma M. Hassan, obtained B.Sc. in computer engineering in 2008, Faculty of Engineering, Department of Electronics and Electrical Engineering Technology, Benha University, Egypt. Graduation Project about “Home Automation Using SMS Control”, Grade of Project is Excellent. Interests studies about cloud computing, Security systems and network

Khaled M. Fouad, obtained B.Sc. in 1995, M.Sc. in 2003 and PhD in 2012, Department of Systems and computers engineering, Faculty of Engineering. Working now as lecturer in Computers and Informatics, Benha University, Egypt, His current research interests focus on Cloud Computing, Big Data, Semantic Web and Expert Systems.

Mahmoud Fathy M. Hassan, had B. Sc. in Electrical Engineering since 1970. His M. Sc. was in Quantum Electronics from Essex University, UK since 1980 and Ph. D. was in Physics of Quantum Electronic from Essex University, UK since 1982. He was appointed as Associate professor in Benha Faculty of Engineering, Benha University, Egypt since 1997. He is currently chairman of Basic Engineering Sciences Department. His research of interests in electronic communications, physics of semiconductor devices and Quantum electronics.