ISSN No. 0976-5697

Volume 3, No. 2, March-April 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Efficient Sending for Iris Biometric Packets through Shortest Reliable Path

Ameer A. Mohammed Baqer*
Department of Computer Engineering, College of Engineering, Bharati Vidyapeeth Deemed University, Pune, India
prof_ameersh@yahoo.com

Suhas H. Patil
Department of Computer Engineering, College of Engineering, Bharati Vidyapeeth Deemed University, Pune, India
shpatil@bvucoep.edu.in

Abstract: Shortest path problem is how finding the shortest path from source to destination in computer networks. The need is to find the path distance from the source to destination which reliable and is found in an optimized way considering the network constraints. One of the basic challenges in distributed systems is how we can send the important packets from one terminal to another through the networks in safety and shortest paths, because sometimes the path is not reliable or the path is long that is take more time to sending the packets, So in our paper we proposed good technique for choosing shortest reliable path to sending Biometric Authentication packet to decrease losing of this packets and also we explain the content of the biometric authentication packet in our proposed web-based system.

Keywords: shortest reliable path; iris biometric authentication; distributed system

I. INTRODUCTION

In reality, the Web represents a huge distributed system that appears as a single resource to the user available at the click of a button. There are several definitions and view points on what distributed systems are. A distributed system is "A system in which hardware or software components located at networked computers communicate and coordinate their actions only by message passing" [1], and another definition for the distributed system as "A collection of independent computers that appear to the users of the system as a single computer" [2]. Leslie Lamport – a famous researcher in distributed systems once said that "A distributed system is one on which I cannot get any work done because some machine I have never heard of has crashed" reflecting on the huge number of challenges faced by distributed system designers.

Various types of distributed systems and applications have been developed and are being used extensively in the real world. In this article, we present one of the main Application of distributed systems that is e-commerce transactions where in this paper we propose a web-based architecture to use encrypted Iris pattern as biometric attribute to authenticate the customer for e-commerce transactions which includes a secure biometric template transmission scheme and we propose good technique to choose shortest reliable path for sending Biometric template through the networks in the form of packets.

II. BIOMETRIC AUTHENTICATION

A biometric authentication virtually eliminates the risk of anonymity in a two factor security scenario by using a physical attribute of the person to authenticate.

Firstly, the requestor presents a token to assert identity. For example, an ATM or credit card is inserted into a reader. (A number encoded on the card is actually the token; the card is more like a container for the token, but treating the card as a token is appropriate.) As with identification, the system must acquire an image of the personal attribute.

Secondly, the attribute must be localized, and a token is formed by integrating the extracted minutiae and a matching template must be generated.

Finally, the value of the token is used to look up the template previously stored. If it matches the requestor is authenticated, Refer to the "Fig. (1)" to above process [3].

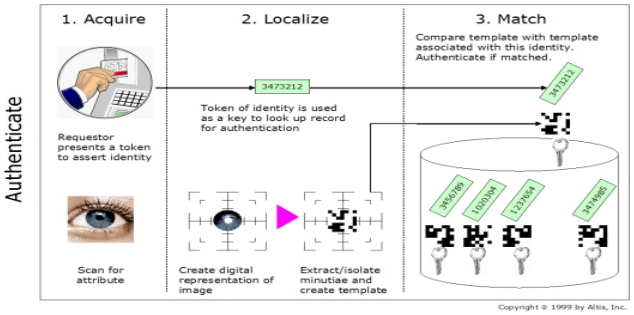


Figure 1: Biometric Authentication Process.

III. BIOMETRIC IRIS-BASED AUTHENTICATION

Having an iris-based authentication system can bring us a list of benefits, for instance [4] [5] [6]

a. Resistance to false matching and exceptionally high levels of accuracy, due to the unique textures of the iris.
b. Stability of characteristic over lifetime, since the iris feature does not change.
c. Suitability for both physical and logical access (in both verification and identification cases).
d. Externally visible and noninvasive to the user, unlike the retina scan.
e. Efficient encoding and search speed (Of course, it depends on the algorithm).

On the other hand, this technology also has its deficiencies, including [5] [7]:

a. Difficulty of usage, since acquisition of the image requires moderate training and attentiveness in the non-automatic systems.
b. False non-matching and failure to enroll. Due to poor image quality of a small moving target, sometimes obscured by eyelashes, lenses, and/or reflections.
c. User discomfort with eye-based technology.
d. Need for a proprietary acquisition device for deployment.

IV. PROPOSED WEB-BASED SYSTEM USING BIOMETRIC AUTHENTICATION

The proposed architecture of the web-based system contains two subsections: Image processing and secure template transmission scheme. In this paper, we are going to propose good technique to choose shortest reliable path for transmitting Biometric Authentication packets. We also explain the content of the biometric authentication packet in our proposed web-based system, as shown in "Fig. (2)".

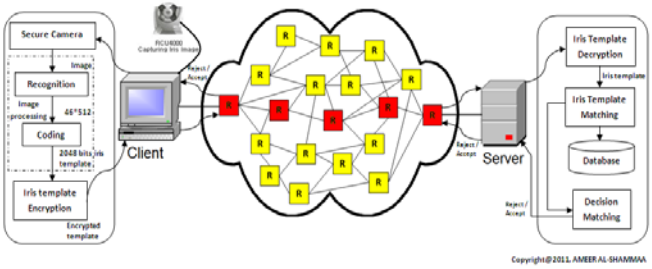


Figure 2: Proposed Web-based system for e-commerce transaction.

In this research, a technical solutions is proposed to prevent the losing biometric authentication packet and decrease the time that is required for sending the packet to destination, also this proposed system used to prevent credit card fraud in e-commerce transactions by using an Iris authentication technique. This method necessitates the existence of standardized Iris image capture and encryption software along with the web camera that is built in the recent computer systems.

Here, iris recognition algorithm is used to extract key characteristic features of Iris pattern of an individual. These features are encrypted using chaotic maps. The result of such a combination provides not only a secure transmission of credit card details, but also achievement of high level authentication. A web-based architecture is proposed for implementing this solution. While issuing a credit card, the Iris details of an individual will be stored along with the credit card number and other personal details in the issuing agency's database [8]. A software need to be present in all the client systems so that while doing e-commerce transactions, the Iris image of the individual can also be captured, encrypted and sent along with the name, credit card number, and expiration date. At the time of transaction the Iris image of the customer is captured using a web camera built in the client system. The Iris image is preprocessed, normalized, enhanced, and the key features of the Iris are extracted using our high performance algorithm, as shown in "Fig. (2)".

A biometric Authentication packet contains two parts:

a. Iris template that is encrypted by chaotic maps.
b. The encryption key that is sent to the server side to decrypt the iris template.

The steps for processing the biometric authentication packets are explained in "Fig. (1)".

V. FINDING SHORTEST RELIABLE PATH

For finding the shortest path, there are many algorithms which already exist. Let us use them and make the suitable shortest path algorithm for finding the shortest reliable path. The routers used OSPF protocol to select the best routes by finding the lowest cost paths to a destination. But it may select a path which is not reliable. The solution to this is OSRPF.

For finding Shortest Reliable path "SRP" follow these steps: [9] [10] [11] [12] [13].

a) Finding all paths from source to destination.
b) Finding reliable paths from available paths.
c) Add one shortest path algorithms to find shortest reliable path.

a. Step one: For finding paths from a graph that has two or more than one node we need search algorithms such as prim's algorithm and save all paths.
b. Step two: For finding reliable path we need to test cables from source to destination each cable has some parameter such as Length, Propagation Delay, Delay skew, resistance, etc.
c. Step three: In this step we should add one algorithm for finding shortest path such as Dijkstra, A*, Floyd's Algorithms, etc.

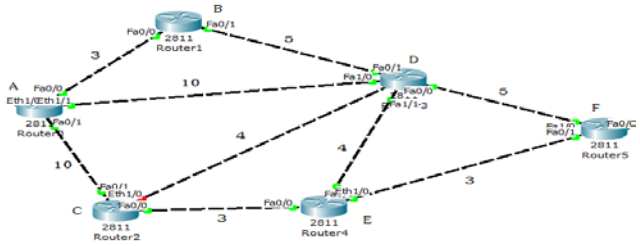
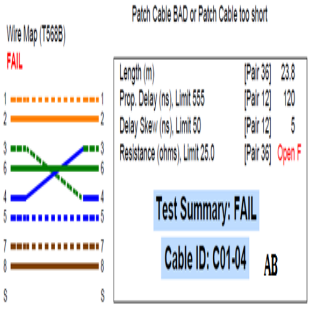
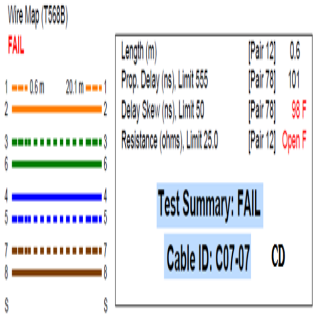


Figure 3: Graphical presentation of paths.

For example after test paths that is shown in "Fig. (3)", we can understand that these edges AB & CD are failed. The results are shown in "Fig. (4)".



Figurers 4a: Test summary for Cable ID C01-04 (PATH: AB)



Figurers 4b: Test summary for Cable ID C07-07 (PATH: CD)

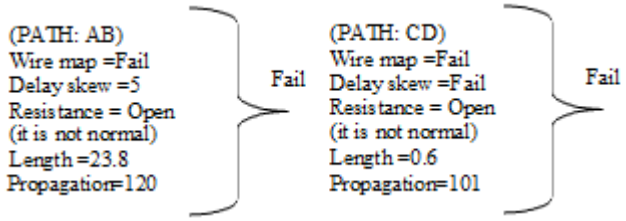


Table I: Paths Result (Fail, Pass)

Path No.	***Path***	***Result***	***Path No.***	***Path***	***Result***
1	ABDF	FAIL	7	ACEF	PASS
2	ABDEF	FAIL	8	ACDF	FAIL
3	ABDCEF	FAIL	9	ACDEF	FAIL
4	ADF	PASS	10	ACDF	FAIL
5	ADCEF	FAIL	11	ACEDF	PASS
6	ADEF	PASS			

We should calculate the cost of 'pass cables' and compare those costs. The path having smallest cost value is best path.

Table I: Cost of Path

Path No.	***Path***	***Result***	***Cost of Path***
4	ADF	PASS	15
6	ADEF	PASS	17
7	ACEF	PASS	16
11	ACEDF	PASS	22

So the shortest reliable path that we can select to send the biometric authentication packet through it is ADF which has a lowest cost.

VI. CONCLUSION

The research work which has been put in this paper is about finding the various shortest reliable paths in the networks and out of that choosing the shortest reliable path for transmitting biometric authentication packet. A model has been proposed for biometric authentication using shortest reliable path.

VII. REFERENCES

[1]. G. Couloris, J. Dollimore, T. Kinberg, "Distributed Systems-Concepts and Design", 4th Edition, Addison-Wesley, Pearson Education, UK, 2001.

[2]. A. Tanenbaum and M. Van Steen,"Distributed Systems: Principles and Paradigms", Prentice Hall, Pearson Education, USA,2002.

[3]. Altis®, Inc., 2011, "Biometric Technology Background", http://www.altisinc.com/resources/Biometric/index.php.

[4]. Ganorkar, S. R., & Ghatol, A. A. "Iris Recognition: An Emerging Biometric Technology". International Conference on Signal Processing, Robotics and Automation, Corfu Island, Greece,2007, pp. 91-96.

[5]. Iridian Technologies. "Iris Recognition Basics, science behind the technology", http://www.iriscan.com.

[6]. Arain R., Sharhriar M., Rozita R. "A New Web-based Architecture Based on Iris Biometrics Technique to Decrease Credit Cards Frauds over Internet". International Journal of Digital Society (IJDS), Vol. 1,2010. pp. 86-93.

[7]. Ratha, N. K., Connell, J. H., & Bolle, R. M. "Biometrics break-ins and band-aids". Pattern Recognition Letters, Vol. 24,2003, pp. 2105-2113.

[8]. International Biometric Group. "Biometric market by technology",2006. http://www.biometricgroup.com.

[9]. Gholamreza Kakamanshadi, J. Naveenkumar, Suhas H. Patil."Hardware Orientation Tests For Establishing Shortest Reliable Path In Computer Networks", International J. of Multidispl. Research & Advcs. in Engg.(IJMRAE), ISSN 0975-7074, Vol. 3, No. IV,2011, pp. (109-116).

[10]. Gholamreza Kakamanshadi, J. Naveenkumar, Suhas H. Patil."A Method To Find Shortest Reliable Path By Hardware Testing And Software Implementation",International Journal of Engineering Science and Technology (IJEST), ISSN: 0975-5462 Vol. 3 No. 7,2011, pp.(5765- 5768).

[11]. www.wikipedia.com/wikifiles/.

[12]. www.openxtra.co.uk/.

[13]. www.flukenetworks.com/.