International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 36 • 2017

Multimodal Biometric Authentication Using Kinect Sensor

A. Saravana Priya[a] and Rajeshwari Mukesh[b]

[a]*Research Scholar, Department of computer science & Engg., St. Peters University, Avadi, Chennai India.*

E-mail: priyaayyavu@yahoo.co.in

[b]*Professor, Department of computer science & Engg., Hindustan Institute of Technology & Science, Chennai, India.*

E-mail: rajeswarim@hindustanuniv.ac.in

Abstract: Security and privacy in any network plays important role for any IT Industry, Smart Home or any social networks. Experts have found many techniques to secure the networks using various Authentication mechanisms. Each mechanism has its own strengths and weaknesses. To enhance the security, this research proposes Multi-modal user Authentication by combining more than one mode of authentication mechanism. This multimodal biometrics are fused together to produce strong and universal authentication. The proposed system authenticates the user by using Microsoft Kinect Sensor device. Kinect sensor plays important role in Biometric authentication where it captures user information by skeleton tracking. Tracked skeleton points are validated on various computations to figure out the person match with existing data record. Authentication fails when there are differences in observed data and data already captured. Proposed system achieved 96% of Accuracy in recognizing the genuine user.

Keywords: *Multiple Authentication, Multi- modal Biometrics, Kinect Sensor.*

1. INTRODUCTION

A Home Area Network (HAN) is used for communication between digital devices generally deployed in home includes multiple pc's, smart phones and other networked home appliances like smart Television, Refrigerator, Washing machine, Air Conditioner etc. All these devices communicate within a Home Network based on trust and store or share any private information. These networks can be connected remote to access these devices from anywhere on the internet. Most accessible devices like personal computers, laptops used for online banking, online shopping and sharing of private information to friend's network or any other network are susceptible to hacks and Intruders to attack.

In most of the Home Networking Technologies, the focus is on device authentication rather than the user authentication which is not reliable to use. User Authentication checks the user credentials supported user request. Multifactor Authentication provides additional privacy for user information in Home network. Multi-factor authentication is truly satisfied by using Biometric Authentication [7]. Users may biometrically authenticate via their fingerprint, voiceprint, palm print, signature, vice recognition etc. and are interoperable with standard authentication mechanism like password, PIN, Security token. Unimodal or static biometrics

reduces the error rate but it cannot resolve the problem [6]. Some of the limitations imposed in Unimodal biometrics can be resolved by multimodal biometrics. Here hard biometric trait like fingerprint, face, iris and ear and soft biometric trait like voice, weight, color etc. are used to enhance the security level.

Kinect is a human motion tracking sensor device to detect the human height, movements, color and audio by using infrared projector and camera. Microsoft free software package development Kit for windows that produce Kinect capabilities to developers to create new applications practicing in Language c, c# using platform Microsoft Visual Studio. The measurements provided by Kinect fluctuate between frames. The accuracy of the system varies from 5% to 10%. User finds more ease of use and universality in using this system.

Kinect includes features like Raw Sensor streams, Skeleton Tracking, Advanced Audio capabilities etc. Capturing the information about the users standing in front of Kinect is Skeleton tracking it need to gain control over the application that interacts with human body motion [12]. Up to six users can be tracked simultaneously and two in detail, which means the sensor, can return all the 20 tracked joint point information. Kinect Sensor can recognize the gesture of the user, voice recognition and facial expressions. Kinect can track more than 40 facial marks of user using Kinect SDK [5].

2. RELATED WORK

2.1. Security with Visual Understanding (SVU)

This paper presents the effective security scheme based on SVU client system. Here Kinect camera monitors the human skeleton form and when a person is detected, SVU validate the person by tracking the skeleton starting from head to toe where nine measurements are taken and compared with data stored in database. Voice command is employed to enter the name of the new person. If a known person is detected, authentication is deemed successful otherwise an audible alarm is notified to the known person mobile as SMS message. The measurements provided by the Kinect fluctuate between frames since the Kinect consider each frame independently of the last. The SVU system has additional a filter to sleek these fluctuations that reduces the false matches [1].

2.2. Dynamic time warping for gesture-based user identification and authentication with Kinect

Kinect is primarily used as gesture driven NUI for motion based controls. Until now, analysis of Kinect based controls preponderantly targets gesture recognition for large base of users. In this paper, the author proposes to use Kinect statistics on exploiting individual gestures. In contrast to devices like facial recognition systems, iris scanners and fingerprint sensors which rely on irrevocable bio-metric information, Kinect based solution offers gesture information as reversible. Author proposes Dynamic Time Warping (DTW) that's based on Kinects ability to detect user's skeletal information for UAM (User access management) [2].

2.3. Tracking of Fingertips and Centers of Palm using KINECT

This paper presents Fingertips detection and centers of palms detection for each hand with use of Microsoft KINECT in 3D space from the given input image. KINECT make process by providing the depth data of foreground objects. Fingertips for one hand are detected and using bended fingers angles values computed in 2D. The hands were metameric using the depth vector and centers of palms were detected with a help of distance transformation used on inverse binary images. This result would be taken as inputs to the robotic hands using hand gesture to reproduce human hands operation [3].

2.4. Wave to Me: User Identification using Body Lengths and Natural gestures

This paper is on user identification using their body segment lengths and natural gestures. It identifies registered user, based on two second hand waving gestures using Kinect device. From the 75 participants with their gesture measurement, performance of the system is evaluated with minimal error rate of 1% [13].

3. SELECTION OF AUTHENTICATION KEY

3.1. Biometrics

In Biometric authentication human physical and behavioral characteristics are used to verify the identity of the user. Biometrics for authentication is comparatively simple to calculate the password strength from its length however strength of biometric shows the issue to quantify the information [5]. Physiological biometric identifiers include fingerprints, hand geometry, ear patterns, eye patterns (iris and retina), facial features, and other physical characteristics. Behavioral identifiers include voice, signature, typing patterns, and others [2]. Multimodal biometric systems resolve the problem of non-universality, since multiple traits guarantee decent population coverage. Further, multimodal biometric systems offer opposed spoofing measures by creating it tough for trespasser to at the same time spoof the multiple biometric traits of a legitimate user [9].

3.2. Kinect Sensor

Kinect may be a line of motion sensing devices that developed a system which will interpret specific gestures, creating utterly hands-free management of electronic devices attainable by associate infrared projector and camera [10]. Microsoft released Software development kit for windows which it provides Kinect capabilities to developers to build applications using c, c# using Microsoft Visual Studio. Kinect include the features like Raw Sensor streams, Skeleton Tracking, Advanced Audio capabilities etc.

Capturing the information about the users standing in front of Kinect is Skeleton tracking. Need to gain control over the application that interacts with human body motion. Users can be tracked up to six people in time and two thoroughly, where the sensor can return all the 20 tracked joint point information. So as to capture the skeleton information initial, have to be compelled to check the Kinect sensor is connected, alter the skeleton stream, attach the event handler for pursuit the skeleton information and begin the Kinect sensor. Once the sensor returns the skeleton information, scan the skeleton frame and map it with UI element [5].

4. PROPOSED SYSTEM USING BIOMETRICS

To explain the Kinect system application thoroughly, consider home appliances that are connected through wired LAN or wireless LAN, where we need, secured transmission of information for managing home appliances using mobile devices within the home or outside of home. The security depends on authentication of every device and all users using them. Authentication provides authorization by assignment access rights and roles to users. For example Head of the Family should be the administrator controlling appliances and network resources for children and visitors. Users should be allowed to temporarily share the data and access data remotely over the cloud. Single factor authentication increases the risk of hacking where people use mobile, like PDA to control home appliance can be stolen by an intruder. Similarly the intruder can get into home and try to access our private data and devices.

In Multiple Biometric authentication, user identification is captured by providing multiple pieces of evidences. Getting input or data from user in more than one way is defined as Multimodal Biometrics. In Multimodal Biometrics, verifying the user credentials on user's request by tracking the posture or gesture of the user and verified against previously collected known user's data. To avoid inherent problems consistently occurred in single biometrics verification, we extend our approach to multimodal fusion biometrics, to achieve higher recognition and performance rate.

The proposed system has been developed using Microsoft Kinect Sensor Camera and Kinect Software development Kit (SDK) which acts as Intrusion detector camera to capture the user and identify them with the help of user dimensions and authenticate them are shown in Fig: 1. It replaces the watch dog activity at home by sensing the unidentified person visiting home. Secondly, family head holds the authority to provide access to the child lock for safety. We focused on skeleton tracking system where every user generally

distinguished over their peers. Initially the Kinect can recognize the human whoever stand in the field view of camera rather than any object are set to ready for tracking the user. Kinect skeleton tracking starts from Center of the Head to foot by identifying their skeleton joints or dimensions where it tracks 20 skeletal joint points all over the body and are collected in all by the proposed system. Each pixel in the image is taken as human body parts. More than one camera can also be used and it can be managed by the Kinect Manager. All the skeleton joints are shown in three Dimensions. In X, Y, Z Space coordinates X and Y are distance between the joints and where Z is the distance from the sensor. Line can be drawn to get the human skeleton picture in 3D space.

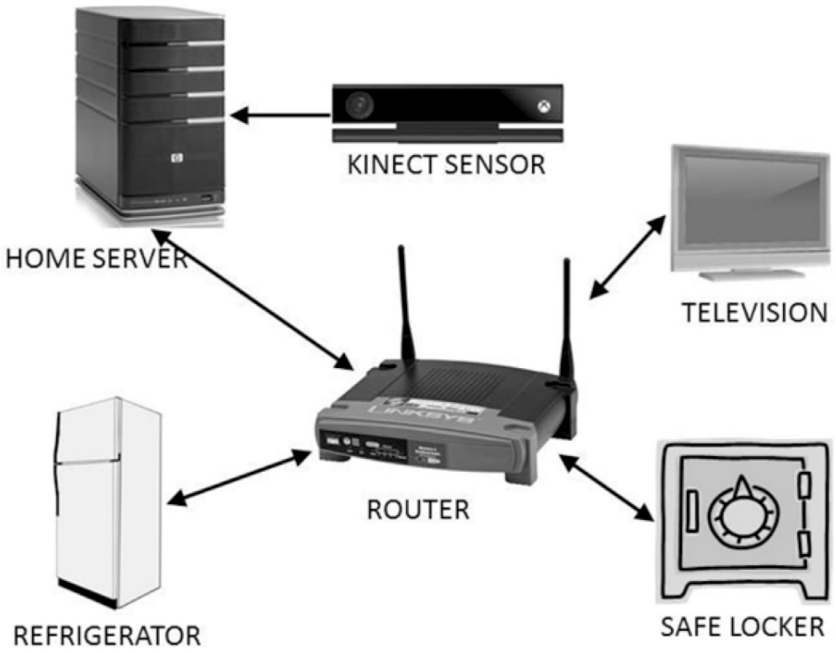

Figure 1: Proposed system Architecture

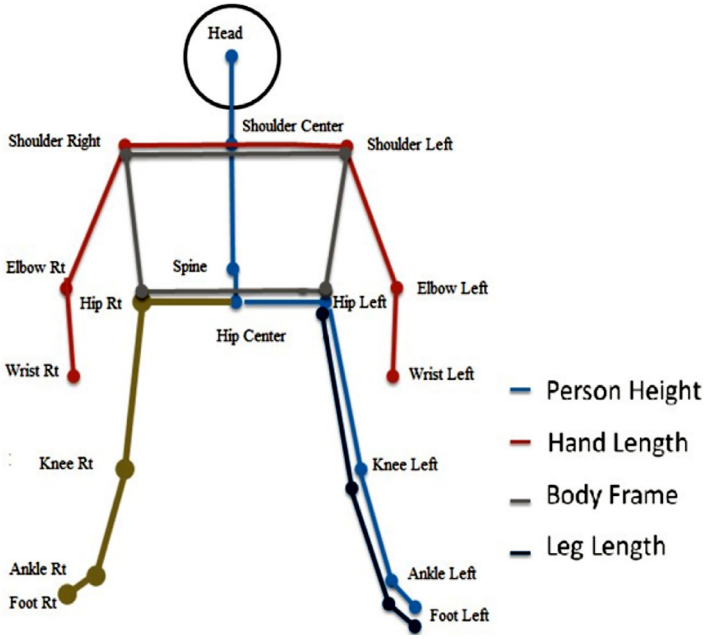

Figure 2: Multimodal biometric Authentication using Kinect (MBAuK) Model

The distance between the joints can be computed using the Euclidean norm (*i.e.*) by finding the square root of the sum of squared differences of the coordinates. To calculate length of two joint points in 3D Space X, Y and Z Coordinates are considered where Z is the depth distance from Kinect and user.

$$e = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2}$$

Distance between skeleton points is calculated as segment lengths to view the skeleton whole body. The system designed to authenticate the user or members in the family by maintaining a database where all family members' skeleton records are registered for first time.

Fig: 2 explains application built to identify the user and authenticate accordingly using Microsoft Kinect device and Kinect Software Development Kit (SDK). When a person is detected, the sensor checks the person's height, person shoulder width, upper part of the body (body frame) and leg length periodically. User Identification considers all the four measurement and compares with already recorded data in dataset for verification. The User Authenticated will be the user who is closest match among the dataset. The flow diagram of user identification and authentication using Kinect are shown in Fig: 3,

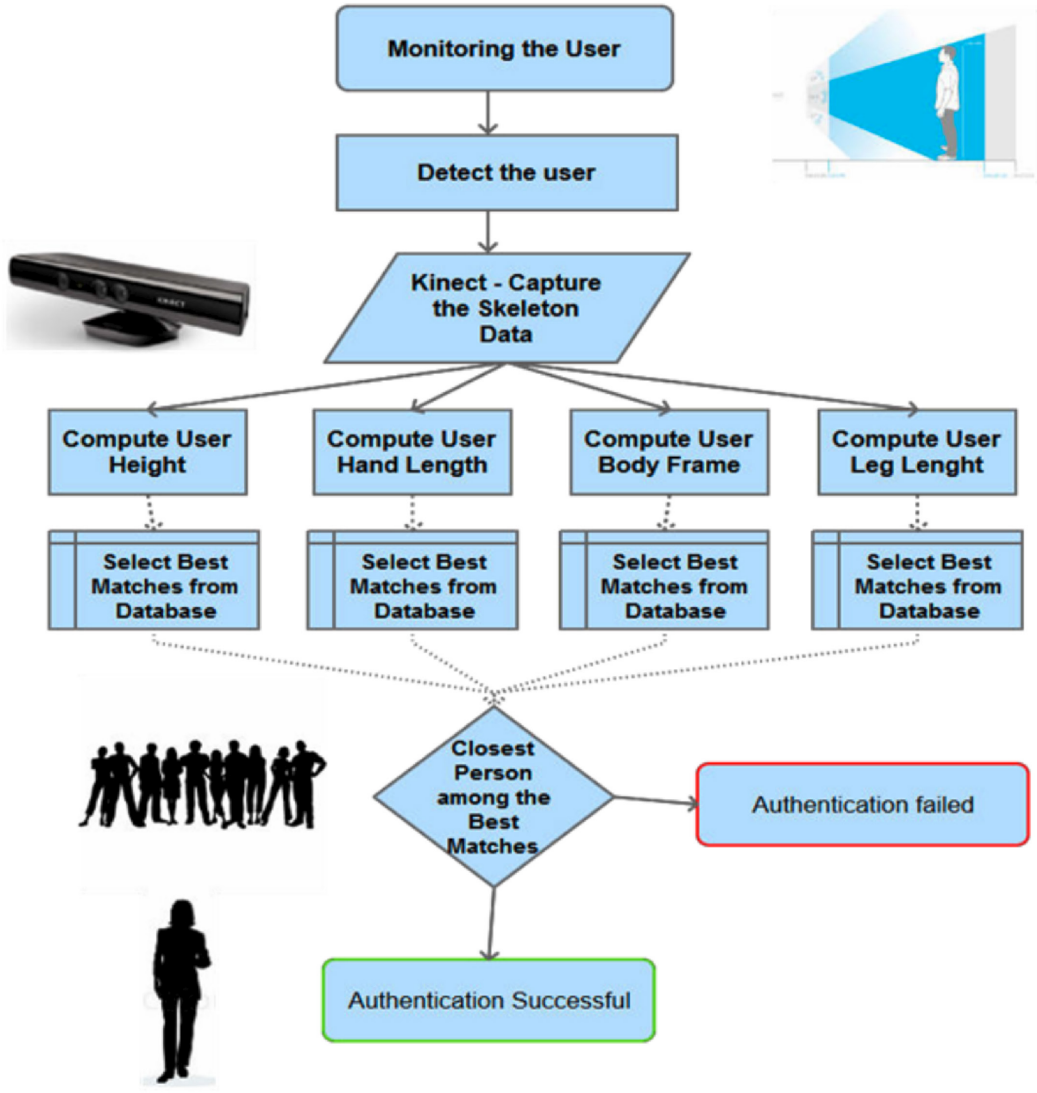

Figure 3: Flow diagram of user identification and authentication in Kinect

For example, to find the height of the person, Kinect starts from the center of head point to foot. Consider the points mentioned below,

Head – Shoulder Center
Shoulder Center – Spine
Spine – Hip Center
Hip Center – Knee Left or Knee Right
Knee Left / Knee Right – Ankle Left / Ankle Right
Ankle Left / Ankle Right – Foot Left / Foot Right

These skeleton points are segmented by Euclidean distance measure and Height of a person is determined by computing set of segment lengths specified for height Δ Height.

$$\Delta \text{ Height} = \sum_{k=0}^{n} \mathrm{H}^{k} \tag{1}$$

Similarly, the length of hand is measured by considering the following Skeleton Dimensions,

Wrist Left – Elbow Left
Elbow Left – Shoulder Left
Shoulder Left – Shoulder Center
Shoulder Center – Shoulder Right
Shoulder Right – Elbow Right
Elbow Right – Wrist Right.

These skeleton points are segmented by Euclidean distance measure and Hand length of a person is determined by computing set of segment lengths specified for Hand Δ Hand Height

$$\Delta \text{ Hand Height} = \sum_{k=0}^{n} \mathrm{H}l^{k} \tag{1}$$

Similarly Body Frame is measured by considering the given Skeleton Dimensions,

Shoulder Left – Shoulder Center
Shoulder Center – Shoulder Right
Shoulder Right – Hip Right
Hip Right – Hip Center
Hip Center – Hip Left
Hip Left – Shoulder left.

These skeleton points are segmented by Euclidean distance measure and Body frame of a person is determined by computing set of segment lengths specified for Body Frame Δ Body Frame,

$$\Delta \text{ Body Frame} = \sum_{k=0}^{n} \mathrm{B}f^{k} \tag{3}$$

Similarly Leg Length is measured by considering the following Skeleton Dimensions,

Hip Left/ Hip Right – Knee Left/ Knee Right
Knee left / Knee Right – Foot Left/ Foot Right.
Foot Left/ Foot Right – Ankle Left/ Ankle Right

These skeleton points are segmented by Euclidean distance measure and Body frame of a person is determined by computing set of segment lengths specified for Leg Length Δ Leg Length,

$$\Delta \text{ Leg Length } = \sum_{k=0}^{n} Ll^{k} \tag{4}$$

Each measurement is compared with the database and finds the best matches among the existing user in the database. All these four measurement periodically checked and shortlists the best matches to minimal. K-nearest algorithm used to find the closest match by computing the test object with the training objects. There is an occurrence of noise in the joint position data which has to be filtered before tracking. There are many smoothing techniques that are available to reduce the noise and jitters from the joints. The Exponential smoothing techniques seems effective to build the application. In Kinect authentication mechanism, accuracy to identify and authorize the person is improved at the maximum.

Algorithm: K-Nearest Neighbor

Input: Data set $Xj \in IRp$. Where $j = 1, 2, 3, 4 \ldots N$ representing data and p represents a point in 3-dimensional space

Process: Calculate distance, $d\,(p', p)$, between test subject (y) and samples in every class, $p \in Xj$.

Select $Xy \subset X\,j$, the set of k closest training objects to y.

Output:
$$y' = \underset{v}{\text{argmax}} \sum (x_k, y_k) \in x_y \, I\,(v = y_k)$$

The Multimodal Biometric Authentication using Kinect, has collected some real data of about 100 samples and accuracy of the system from the registered user are shown in Fig:4. In graph analysis structure we could see there is a narrow gap that exists between each user which defines their identity in nature.

Biometric Skeleton trait	*Registered Users for training #*	*Algorithm*	*Person Recognition Rate %*
Body Height	25	K-Nearest Neighbor	96.5
	50		95.9
	75		95.4
	100		95.2
Body frame	25		96.2
	50		96.0
	75		95.9
	100		95.9
Hand Length	25		96.9
	50		96.7
	75		96.7
	100		96.5
Leg Length	25		96.8
	50		96.8
	75		96
	100		96.2

Figure 4: Accuracy of the classification system obtained from the registered users

Multimodal Biometric Authentication using Kinect system is a real time application which identifies the user and authenticates accordingly. Fig: 5 it provides Kinect capabilities to developers to build applications are the application screenshot taken where Kinect authenticates the user by skeleton tracking. The application displays all the measurement taken for the user and closest person detected with lowest difference found among the best matches in the dataset.

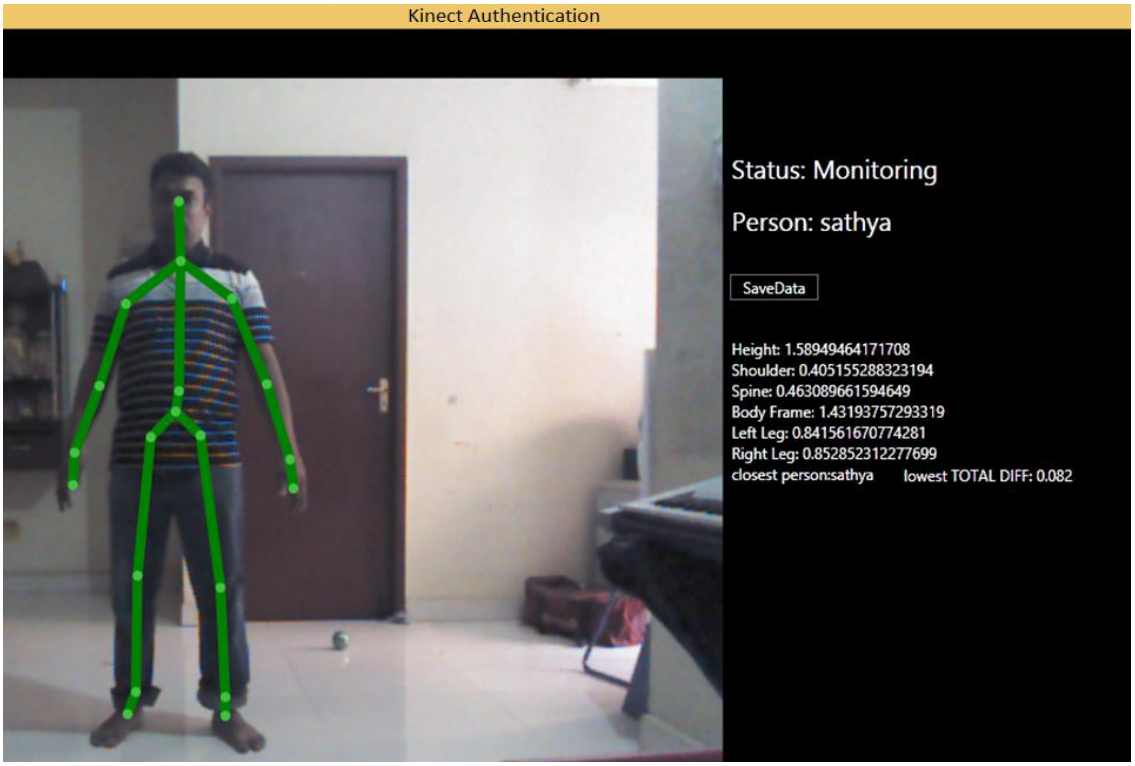

Figure 5: Kinect authenticate the user by skeleton tracking.

When the person cannot be identified against the known list, the application shows the status as unknown. Fig: 6 show the person is unknown to the Kinect and hence user stands unauthenticated.

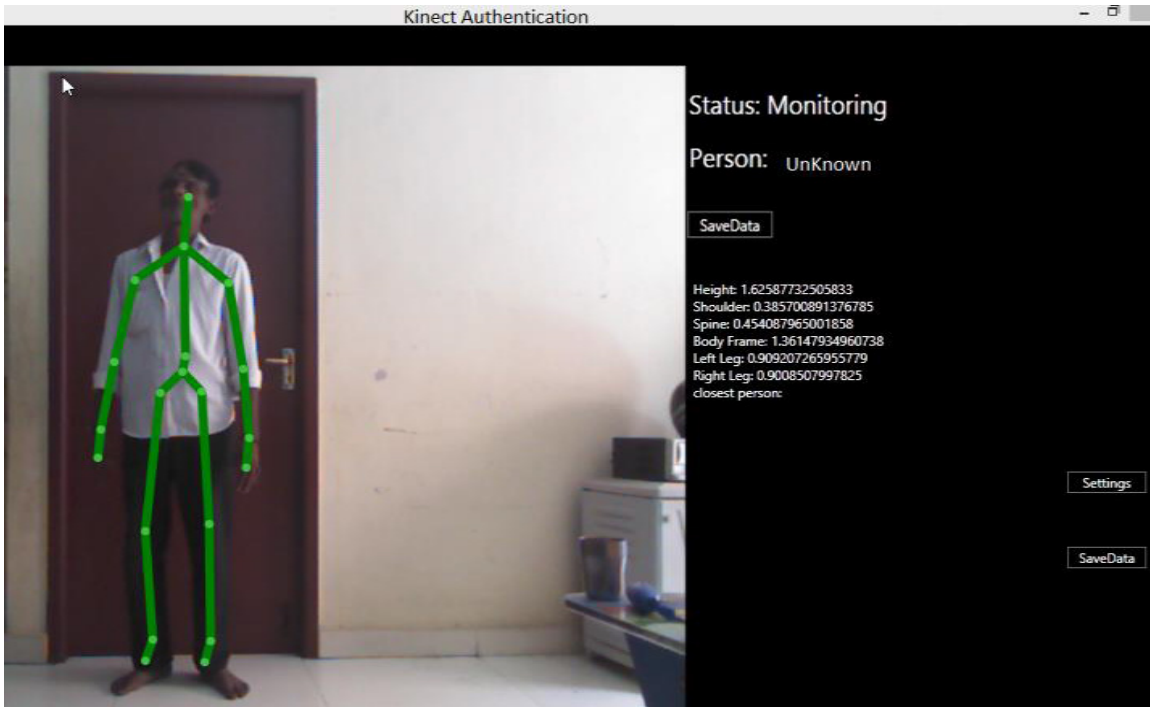

Figure 6: Unknown User to Kinect

5. LIMITATIONS

Kinect finds it difficult to track skeleton joints when user wears traditional clothes like saree and clothes that mask full body structure. This model requires Kinect to be available at user's location to authenticate them and hence cannot be used to authenticate remote users.

6. CONCLUSIONS

This paper describes about Multifactor Authentication on Home Network devices using multimodal biometrics using Kinect sensor device. Strong identification, verification and authorization can prevent threats to home networks from intruders, friends and visitors. Home user can use this system with more convenient and non – intrusive way. System focused on strong authentication as well more ease of use by the user.

REFERENCES

[1] S. Joseph Fluckiger, "Security with Visual Understanding: Kinect Human Recognition Capabilities Applied in a Home Security System", White Paper, 2012.

[2] Wu. J Dept. of Electrical and Computer. Eng., Boston Univ., Boston, MA, USA Konrad, Ishwar, P, "Dynamic time warping for gesture-based user identification and authentication with Kinect", IEEE International Conference on May 2013.

[3] Raheja , J.L and Chaudhary, A. ; Singal. K "Tracking of Fingertips and Centers of Palm using KINECT" Third International Conference on 20 -22 Sep 2011.

[4] Sinha, A. ; Innovation Lab., Tata Consultancy Services Ltd., Kolkata, India Chakravarty . K., "Pose Based Person Identification Using Kinect", IEEE International Conference on Oct 2013.

[5] Abhijit Jana," Kinect for Windows SDK Programming Guide" Ch6: Skeleton Tracking.

[6] Wikipedia [http://en.wikipedia.org]: Home Networks.

[7] Wikipedia [http://en.wikipedia.org]: Bio-metrics

[8] Wikipedia [http://en.wikipedia.org]: Multi-factor authentication.

[9] A. Ross and A. K. Jain, "Information fusion in biometrics," Pattern Recogn. Lett, vol. 24, no. 13, pp. 2115–2125, Sep. 2003.

[10] S. Imran Ansari, S. Ahmad Qutbuddin, "Biometrics for home security", Electrical and computer Engineering, proceedings of 2009 IEEE student conference on Research and Development.

[11] Heikki Kalviainen, Jussi Parkkinen, Arto Kaarna(Eds) "Image Analysis" Springer 14th Scandinavian Conference, SCIA 2005 Proceedings.

[12] Wikipedia [http://en.wikipedia.org/wiki/Kinect]

[13] Eiji Hayashi, "Wave to me: User Identification using Body Lengths and natural gestures", ACM, 2014.