Remote Health Monitor, Security Issues,
Multi-Factor Biometric Authentication,
Keystroke Analysis, Face Recognition

Tapalina BHATTASALI[1], Khalid SAEED[2], Nabendu CHAKI[1], Rituparna CHAKI[3]

BIO-AUTHENTICATION FOR LAYERED REMOTE HEALTH MONITOR FRAMEWORK

Aged people, patients with chronic disease, patients at remote location need continuous monitoring under healthcare professionals. Remote health monitor is likely to be an effective approach to provide healthcare service in a simple and cost effective way. However, effective implementation of this type of framework needs consideration of variety of security threats. In this paper, a layer based remote health monitor framework is proposed to analyze health condition of patients from remote places. Beside this, a multi-modal biometric authentication mechanism is proposed here to reduce misuse of health data and biometrics templates in heterogeneous cloud environment. Main focus of the paper is to design semi-continuous authentication mechanism after establishing mutual 1:1 trust relationship among the participants in cloud environment. Behavioral biometrics keystroke analysis is fused with physiological biometrics face recognition to enhance accuracy of authentication. Instead of considering traditional performance evaluation parameters for biometrics, this paper considers a few performance metrics for determining efficiency of semi-continuous verification of the proposed framework.

1. INTRODUCTION

Remote health monitor provides healthcare service for patients from remote locations to support various cases such as chronic disease management, assisted aged living. It has the potential in positive medical outcome as well as in cost-effectiveness over traditional healthcare. To provide ubiquitous connectivity in “any” paradigm, remote health monitor framework should support integration of medical devices, huge amount of sensitive data, end-users, various processes and services with heterogeneous technologies. Pervasive nature of remote health makes it easy for malicious adversaries to launch security threats [4], [7]. Identification of security threats in this domain is still an open research issue. Secure access of Electronic Health Record (EHR), Electronic Medical Record (EMR), and Personal Health Information (PHI) stored in cloud like third party distributed domain is a challenging task. One of the major security challenges [13] of remote health monitor framework is loss of authenticity, where anyone can access patient’s data without giving any validity proof. It may result into loss of confidentiality, where patient’s privacy become vulnerable. It also results into loss of integrity, where alteration to health data leading to incorrect diagnosis and treatment and loss of availability, which in turn results into insufficient treatment of patients [9]. As remote health services are designed to assist in medical treatment, security vulnerabilities lead the entire system unreliable, putting patients at risk. Security solution of remote health framework must be compatible with existing remote healthcare regulations and standards such as HIPAA [5], HL7 PASS model [6]. There is no significance of considering healthcare application excluding security concept. Research in this area from security perspective is still at very early stage.

[1] Department of Computer Science nd Engineering, University of Calcutta, JD -2,Sector -III, Saltlake City, Kolkata, India
[2] Faculty of Computer Science, Bialystok Institute of Technology, 45A, Wiejska Street, 15-351 Bialystok, Poland
[3] A. K. Chaudhury School of Information Technology, University of Calcutta, JD -2, Sector -III, Saltlake City, Kolkata, India

The major focus should be given first on secure authentication mechanism to control access of sensitive health data. Existing security solutions can not address all the challenges that may appear in remote health framework. This proposal focuses on most of the security specific requirements in remote health application such as simplicity, cost-effectiveness, reliability, semi-continuous verification, accuracy, fast response.

The main contribution of this work is to design effective layer based remote health monitor framework in heterogeneous environment and to propose trust based multifactor bio-authentication mechanism without compromising the purpose of proposed framework. The objective of designing layer based remote health monitor framework is to reduce cost and complexity and to enhance throughput and scalability. A novel multi-biometric authentication mechanism (multifactor) is considered here to enhance reliability over traditional mechanisms. The rest of the paper is organized as follows. Section 2 introduces proposed framework of remote health monitor. Section 3 represents a novel authentication mechanism based on fusion of behavioral biometrics (keystroke analysis) and physiological biometrics (face recognition) for the proposed remote health monitor framework. Section 4 briefly presents the analysis part. Section 5 concludes the paper.

2. PROPOSED LAYERED REMOTE HEALTH MONITOR FRAMEWORK

In this section, a brief idea about the layer based Remote Health Monitor framework is given. Figure 1 represents proposed remote health monitor framework. Proposed remote health monitor framework is partitioned into six layers - Sensing layer, Data collection layer, Transport layer, Processing layer, Application layer, Transaction layer. A brief overview of different components of layered remote health monitor framework is given in Figure 2. Basic activities of the proposed framework are given here. Initially end-users (patients, doctors, caregivers etc.) need to be registered through biometric user interface to remote health monitor service provider to generate user-ID. Bio-medical sensors sense biological parameters such as heart rate, blood pressure etc from the patient's body. Smart sensing nodes capture events from daily activities of the patients and send it towards data aggregator (e.g., smart phones). Dynamic and energy-efficient pull model of data aggregator is considered that selectively pulls required sensor data instead of receiving continuous flow of sensing data. Filtered data are transmitted towards remote health monitor service provider (web-server) through edge router. Remote health monitor service provider consults with authentic healthcare experts for preparation of EMR, EHR, and PHI by analyzing basic behavioral pattern of patients using context management system. Any deviation in health records of patients is analyzed to determine whether emergency situation occurs or not. During

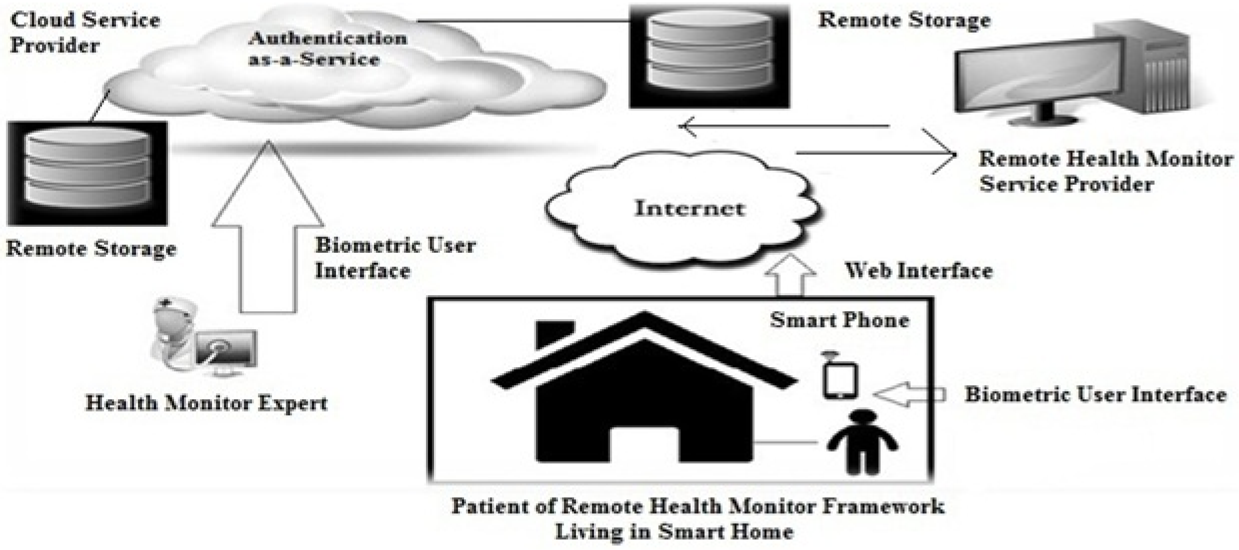
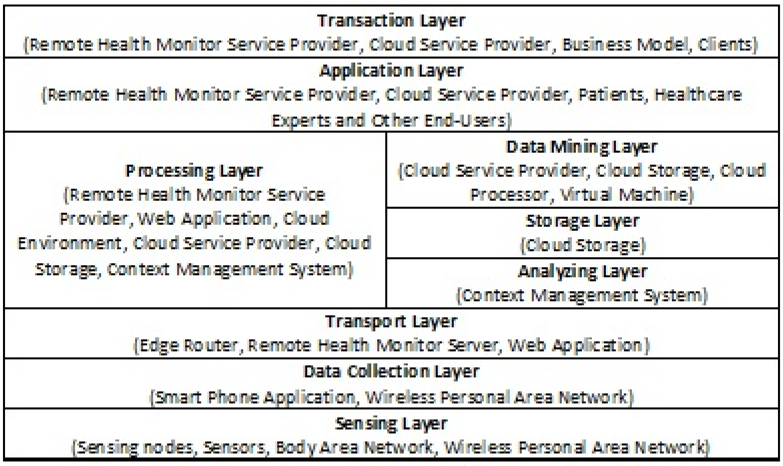


Fig. 1. Proposed Remote Health Monitor Framework.



Transaction Layer
(Remote Health Monitor Service Provider, Cloud Service Provider, Business Model, Clients)
Application Layer
(Remote Health Monitor Service Provider, Cloud Service Provider, Patients, Healthcare Experts and Other End-Users)
Processing Layer
(Remote Health Monitor Service Provider, Web Application, Cloud Environment, Cloud Service Provider, Cloud Storage, Context Management System)
Data Mining Layer
(Cloud Service Provider, Cloud Storage, Cloud Processor, Virtual Machine)
Storage Layer
(Cloud Storage)
Analyzing Layer
(Context Management System)
Transport Layer
(Edge Router, Remote Health Monitor Server, Web Application)
Data Collection Layer
(Smart Phone Application, Wireless Personal Area Network)
Sensing Layer
(Sensing nodes, Sensors, Body Area Network, Wireless Personal Area Network)

Fig. 2. Components of Proposed Six Layer Remote Health Monitor Framework.

emergency, alert is triggered to provide immediate actions from remote health monitor service provider site. For minor events, warning goes towards all valid end-users of the framework. Remote health service provider uses cloud environment to store huge amount of sensitive data of patients in a cost-effective and less complex way. Healthcare experts or caregivers can directly access health related data of patients from cloud according to their access rights regularly via biometric interface, where authentication is provided as a service.

3. TRUST BASED FUSED BIO-AUTHENTICATION MECHANISM FOR PROPOSED REMOTE HEALTH

In proposed remote health monitor framework, any interaction between two entities (human to human, human to machine, machine to machine) needs valid authentication proof. For this reason, authentication mechanism is proposed here to ensure that stored sensitive data are allowed to be accessed only by valid entities and CIA (confidentiality-integrity-availability) concept is preserved. In this paper, primary focus is given on trust based bio-authentication technique to validate healthcare experts and to enhance reliability of the mechanism. Some of the limitations of unimodal authentication are overcome here by fusing multiple modes or factors. Figure 3 represents trust based authentication concept.

Sensitive data (health records, biometric templates) are kept on trustworthy cloud servers and one to one (1:1) trust relationship is established between the cloud users (cloud service consumer, cloud service provider) based on the following issues [3][7].

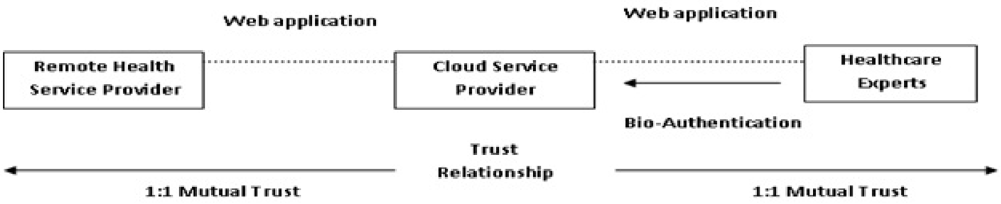


Fig. 3. Trust based Bio-Authentication for Remote Health Monitor Framework.

- No access of encrypted data stored at cloud storage by malicious users as well as cloud service provider;
- Secure transfer of critical data to and from cloud service provider (based on Transport Layer Security protocol) end;
- Updated data should always be available for the authentic cloud users;

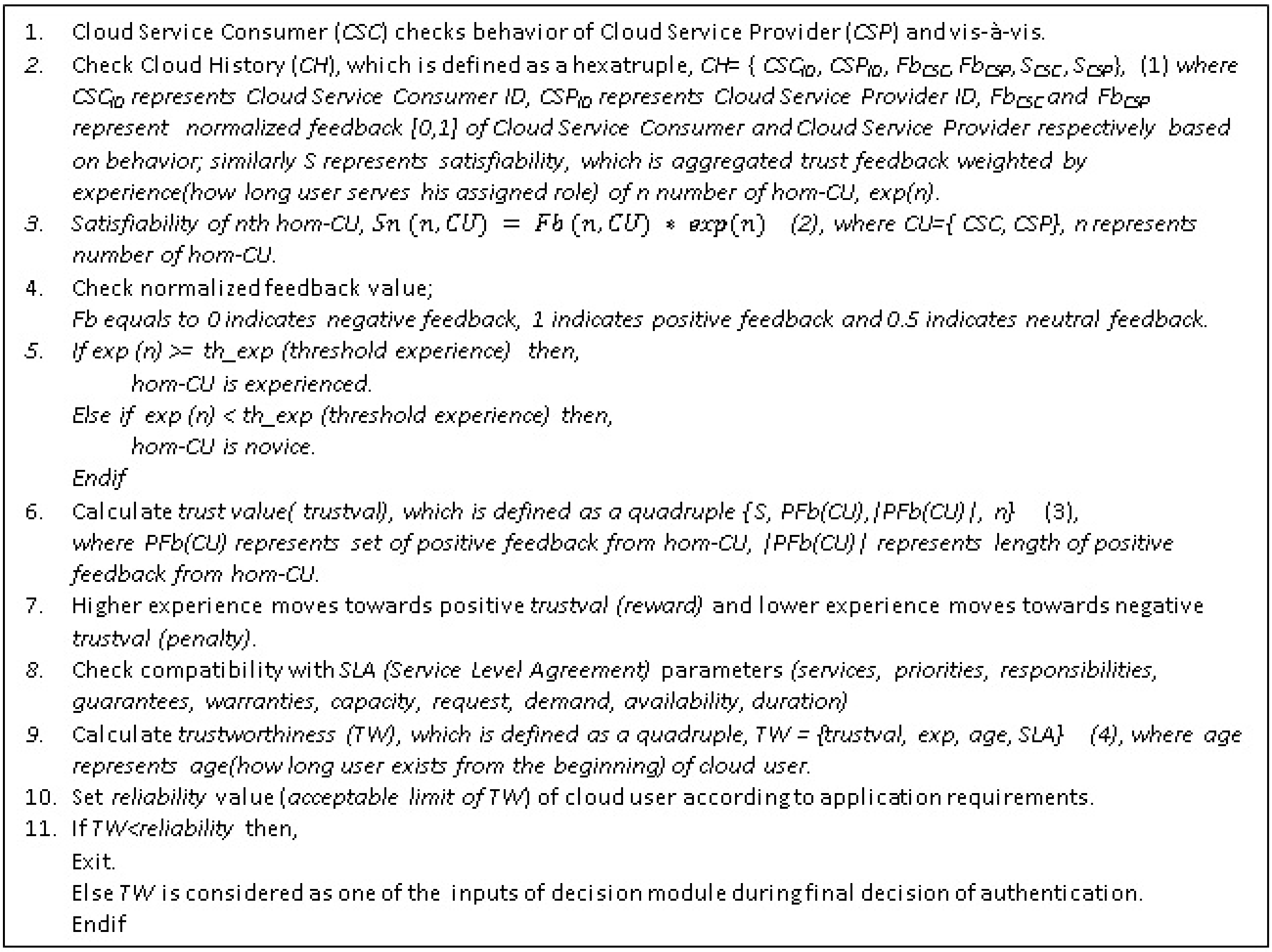
Cloud service provider provides cloud service on pay per use basis, whereas cloud service consumer (healthcare experts, remote health monitor service provider) consumes service. In trust based bio-authentication service, mutual trust is established between service provider and service consumer (health-care experts) [3] along with valid authentication proof. Same category cloud users (*CU*) are known as *hom-CU*, different categories cloud users are known as *het-CU*.

Proposed bio-authentication model is considered as multifactor authentication model (end-user, device, service). End-user authentication is based on biometrics data, whereas device authentication is based on device -id and IP address and service authentication is based on assigned access rights and role of the end-users. As biometric traits cannot be lost or forgotten, biometric authentication provides a solution to ensure that the desired services are accessed only by a valid end-user. No single biometrics is capable to meet all the requirements of every application. The major concern of biometric authentication is false positive and false negative detection, where either unauthorized users are granted access permission or valid users are blocked to access data. Another challenge arises when a session of valid user is hijacked by impostor during static authentication (where authentication is only at the beginning of the session). For this reason, semi-continuous authentication is considered here, where user is verified repeatedly throughout the lifetime of the session. Authentication model in cloud environment works in registration phase, and verification phase. During registration for a service, a cloud user registers with his unique traits along with the device he uses. These get stored as templates at the cloud service provider's end. Every time when an access is made, the cloud user is prompted to provide his registered trait that is compared against the template and authenticated accordingly. User verification occurs at the following times.

- User first enters into the system for a claimed identity;
- User does not interact with system for a long time;
- After a pre-defined time interval;
- After any unusual behavior monitored;

Data access can be blocked in the middle of the session if any unusual event is noticed by the system. Trust model is considered here to reduce the probability of intrusion by impostors. Figure 4 represents basic overview of trust model. Behavioral biometrics Keystroke analysis [11] provides a cost-effective solution for cloud based remote health application [2] due to the fact that it does not require any additional hardware. It becomes popular among other behavioral biometrics, because of its high portability over the Internet, and its simplicity. It is used to identify users uniquely by utilizing the rhythm and manner in which an individual types characters on a keyboard. Fixed text (password) timing data are normally used during initial login and free texts are used for semi-continuous monitoring that checks whether impostor has taken control over the valid user. However, keystroke analysis may not give accurate result alone, because of its low repeatability. For this reason, physiological biometrics face recognition [8], [10], [14] is fused with keystroke analysis at matching score level. The reason behind considering face recognition is that it is also cheaper as it only requires camera (webcam) to capture biometric traits. Figure 5 represents logic of fused bio-authentication model. End user authentication includes login information (password), timing data of fixed texts as well as free texts, and face images of end-users. This type of authentication model is capable to alter itself to acceptable changes according to the behavior or acceptable physical changes of the user. Each biometrics works in parallel upto match module and evaluates match score. Then match scores are fused to evaluate final match score. Multimodal end-user authentication is presented in Figure 6. Fused bio-authentication mechanism steps are given below briefly.

- **Keystroke Analysis: Raw data collection** - Application collects raw typing data [2][11] from the end-users. It submits following information to the web server- keys pressed and time stamps of the key events [2], [11], date and time of submission.
- **Feature extraction** - Average key latency is calculated for each typable n-graph of users. Temporal data are clusterized according to modified k-mean algorithm on the basis of usage frequency.
- **Outlier remova**l - Outliers of the extracted features are detected to remove noisy data by using standard deviation method [1].



1. Cloud Service Consumer (*CSC*) checks behavior of Cloud Service Provider (*CSP*) and vis-à-vis.
2. Check Cloud History (*CH*), which is defined as a hexatruple, *CH*= { CSC_{ID}, CSP_{ID}, Fb_{CSC}, Fb_{CSP}, S_{CSC}, S_{CSP}}, (1) *where CSC_{ID} represents Cloud Service Consumer ID, CSP_{ID} represents Cloud Service Provider ID, Fb_{CSC} and Fb_{CSP} represent normalized feedback [0,1] of Cloud Service Consumer and Cloud Service Provider respectively based on behavior; similarly S represents satisfiability, which is aggregated trust feedback weighted by experience(how long user serves his assigned role) of n number of hom-CU, exp(n).*
3. *Satisfiability of nth hom-CU, $Sn\ (n, CU) = Fb\ (n, CU) * exp(n)$ (2), where CU={ CSC, CSP}, n represents number of hom-CU.*
4. Check normalized feedback value;
   Fb equals to 0 indicates negative feedback, 1 indicates positive feedback and 0.5 indicates neutral feedback.
5. *If exp (n) >= th_exp (threshold experience) then,*
   hom-CU is experienced.
   Else if exp (n) < th_exp (threshold experience) then,
   hom-CU is novice.
   Endif
6. Calculate *trust value(trustval), which is defined as a quadruple {S, PFb(CU), |PFb(CU)|, n}* (3), *where PFb(CU) represents set of positive feedback from hom-CU, |PFb(CU)| represents length of positive feedback from hom-CU.*
7. Higher experience moves towards positive *trustval (reward)* and lower experience moves towards negative *trustval (penalty).*
8. Check compatibility with *SLA (Service Level Agreement)* parameters *(services, priorities, responsibilities, guarantees, warranties, capacity, request, demand, availability, duration)*
9. Calculate *trustworthiness (TW), which is defined as a quadruple, TW = {trustval, exp, age, SLA}* (4), *where age represents age(how long user exists from the beginning) of cloud user.*
10. Set *reliability* value (*acceptable limit of TW*) of cloud user according to application requirements.
11. If *TW<reliability* then,
    Exit.
    Else *TW* is considered as one of the inputs of decision module during final decision of authentication.
    Endif

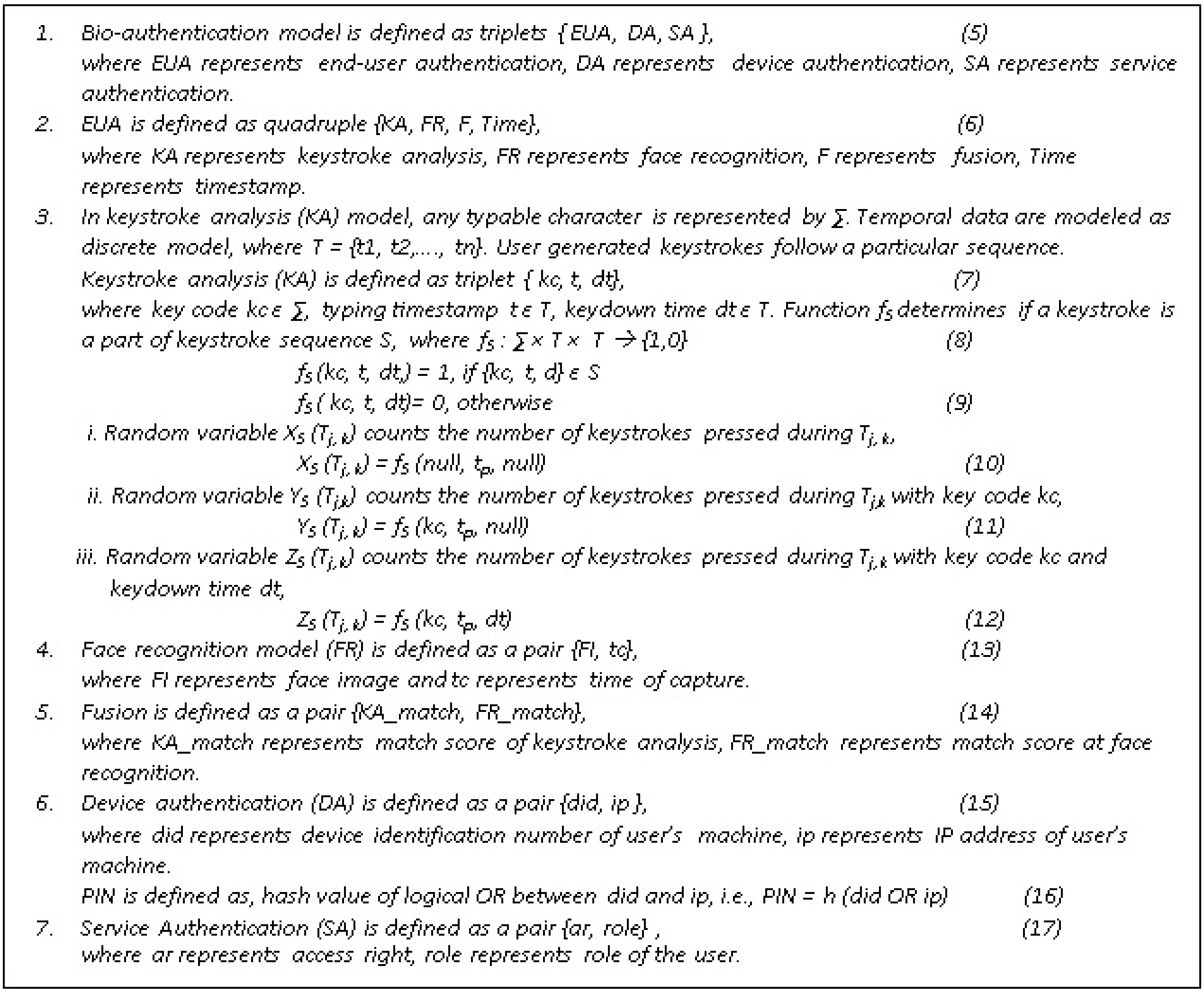
Fig. 4. Basic Overview of Trust Model.

- **Data normalization** - Data are normalized according to minmax algorithm [1].
- **Training of data -** Collected input patterns are transmitted to the neural network model to compute actual output by updating incoming network weights and continues until all data are submitted.
- **Template generation** - Template stores valid reference signatures of authentic users based on timing data and network weights for keystroke model. Temporal data of frequently used typing patterns are normally considered for template generation to distinguish between a legitimate user and an impostor.
- **Testing of data** - If learning of the model is completed, testing phase is used to check whether submitted input data is matched with previously stored template data. Trained neural network verifies test data to generate classifier decision accurately.
- **Match module** - Match logic evaluates match score on the basis of classification accuracy, weight and biasness of the network.

$$r = avgdeviation \times biasness \tag{1}$$

If classifier identifies any test object as valid (if r is within threshold limit t),then positive match (binary 1) is assigned. Otherwise, if test object is identified as invalid, then negative match (binary 0) is assigned. Average deviation represents closeness of user's pattern in a session to the valid user.

$$avgdeviation = \frac{1}{N}\left(\frac{\sum_{i=1}^{N}|patti - Patterni|}{Patterni}\cdot 100\right) \tag{2}$$



1. Bio-authentication model is defined as triplets { EUA, DA, SA }, (5)
where EUA represents end-user authentication, DA represents device authentication, SA represents service authentication.
2. EUA is defined as quadruple {KA, FR, F, Time}, (6)
where KA represents keystroke analysis, FR represents face recognition, F represents fusion, Time represents timestamp.
3. In keystroke analysis (KA) model, any typable character is represented by ∑. Temporal data are modeled as discrete model, where T = {t1, t2,...., tn}. User generated keystrokes follow a particular sequence.
Keystroke analysis (KA) is defined as triplet { kc, t, dt}, (7)
where key code kc ϵ ∑, typing timestamp t ϵ T, keydown time dt ϵ T. Function f_S determines if a keystroke is a part of keystroke sequence S, where $f_S : \sum \times T \times T \rightarrow \{1,0\}$ (8)
f_S (kc, t, dt,) = 1, if {kc, t, d} ϵ S
f_S (kc, t, dt)= 0, otherwise (9)
i. Random variable X_S ($T_{j,k}$) counts the number of keystrokes pressed during $T_{j,k}$,
X_S ($T_{j,k}$) = f_S (null, t_p, null) (10)
ii. Random variable Y_S ($T_{j,k}$) counts the number of keystrokes pressed during $T_{j,k}$ with key code kc,
Y_S ($T_{j,k}$) = f_S (kc, t_p, null) (11)
iii. Random variable Z_S ($T_{j,k}$) counts the number of keystrokes pressed during $T_{j,k}$ with key code kc and keydown time dt,
Z_S ($T_{j,k}$) = f_S (kc, t_p, dt) (12)
4. Face recognition model (FR) is defined as a pair {FI, tc}, (13)
where FI represents face image and tc represents time of capture.
5. Fusion is defined as a pair {KA_match, FR_match}, (14)
where KA_match represents match score of keystroke analysis, FR_match represents match score at face recognition.
6. Device authentication (DA) is defined as a pair {did, ip }, (15)
where did represents device identification number of user's machine, ip represents IP address of user's machine.
PIN is defined as, hash value of logical OR between did and ip, i.e., PIN = h (did OR ip) (16)
7. Service Authentication (SA) is defined as a pair {ar, role} , (17)
where ar represents access right, role represents role of the user.

Fig. 5. Fused Bio-Authentication Model.

where N is the total number of data set, patti is average key latency for the ith sample in user's session, Patterni is reference signature resulting from user's template. Lower number represents high probability of closeness to ensure that session belongs to the same user.

- **Face Recognition: Raw data collection** - Application captures face image [12], [14] from the end-users by webcam and raw image is submitted to the web server.
- **Feature extraction -** Gabor wavelet representation [14] is extracted from raw face image. Principle Component Analysis (PCA) is used to reduce dimensions of data set and to compute Eigen value decomposition for better performance recognition.
- **Outlier removal**- Noisy faces are filtered out during training phase as well as during verification phase.Histogram equalization and background removal are used to improve face recognition performance.
- **Template generation -** For each acquired face, template database stores the image itself as well as weight vectors computed at training phase (using PCA technique).
- **Match module -** Normalized Euclidean distance between two feature vectors is used to determine closeness between valid user and claimed identity (using PCA technique) to evaluate match score.
- **Multimodal: Normalization of match score and Fusion -** Individual match score generated by each biometrics model is mapped into a common domain. Match scores are normalized by minmax algorithm [1] to a range of [0,1].Normalized match score is fused by simplest fusion method- weighted sum, having low computational cost [14].
- **Decision module**- Decision module evaluates final decision by fusing match score and *trustwor-*

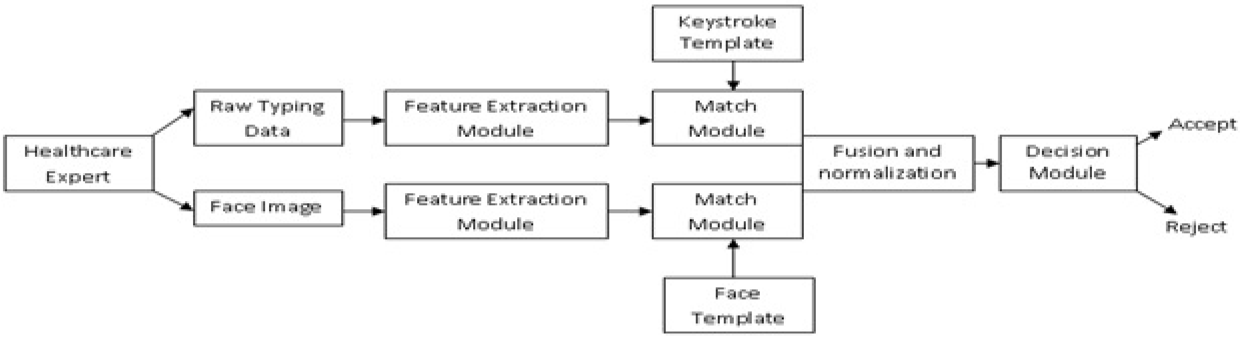


Fig. 6. Multimodal End-User Authentication.

thiness (tw) of the user.

$$\begin{gathered} if\ decision\,(fusedmatch, tw)\ >\ = thtolerate\ then \\ end - user\ is\ treated\ as\ authentic\ healthcare\ expert. \end{gathered} \tag{3}$$

$$\begin{gathered} if\ decision\,(fusedmatch, tw)\ < thtolerate\ then \\ end - user\ is\ treated\ as\ authentic\ healthcare\ impostor. \end{gathered} \tag{4}$$

,where *thtolerate* represents threshold limit of tolerance.

4. Analysis

Performance metrics of false accept and false reject rates are not always capable to evaluate sufficient result for semi-continuous verification in remote health monitor framework. In real time semi-continuous verification, time is a major concern. Some parameters are considered here to analyze the overall performance of remote health monitor framework.

- **Time to True Reject (*TTR*)** - It is defined as the time gap between the first activity of impostor and a time period, when system truly rejects user as the impostor.

$$Time\ to\ True\ Reject(TTR) = |TFIMP - TRIMP| \tag{5}$$

  where *TFIMP* represents timestamp of first activity of impostor and *TRIMP* represents timestamp when system truly rejects impostor. It is used to determine how fast semi-continuous authentication mechanism detects impostor's activity in the framework. *TTR* is measured in seconds. Ideally *TTR* should be zero. If system fails to reject the impostor truly, *TTR* moves towards infinity. In reality, *TTR* should be less than a vulnerability-frame (minimum time required by the impostor to damage the system) to guarantee system integrity. However, this time is application specific.
- **Validity -** For valid users, validity is defined as the fraction of the duration, when user is granted an access to resource and total log-in time. During log-in session (*T seconds*), valid user is either accepted or rejected. If *t* is a duration, when the user is accepted by the system, then

$$validity = \frac{t}{T} \tag{6}$$

  This concept is similar to *true acceptance rate (TAR).*
- **Probability Time to True Reject (*PTTR*) -** Ideally, *Prob* (*TTR* > *vulnerability-frame*) should be equal to 1. Sometimes it can take longer time than vulnerability-frame (seconds) to truly reject impostor, when *Prob* (*TTR*) < 1, that is tolerable. If system always fails to reject impostor within vulnerability-frame, then *PTTR* is equal to zero for all vulnerability frames. This is similar to false acceptance rate (*FAR*).
- **Validity-Acceptability Characteristic Curve (*VACC*)** - Semi-continuous verification system accepts or rejects end-users based on some threshold levels. Curve of validity versus *PTTR* gives rise to Validity-Acceptability Characteristic Curve (*VACC*). This is similar to *ROC curve* used

to measure accuracy of one-time verification. Area under *VACC* is used to measure the overall performance of a semi-continuous authentication system.

Performance analysis of the proposed authentication mechanism is given below briefly on the basis of the above mentioned performance metrics. Datasets used for the analysis are based on some specific cases that may appear in semi-continuous authentication system. All users excluding valid one are considered as impostors during performance analysis. Initially, any random activity of invalid user is considered as first activity of impostor. The moment when impostor is accurately detected by the system is recorded.

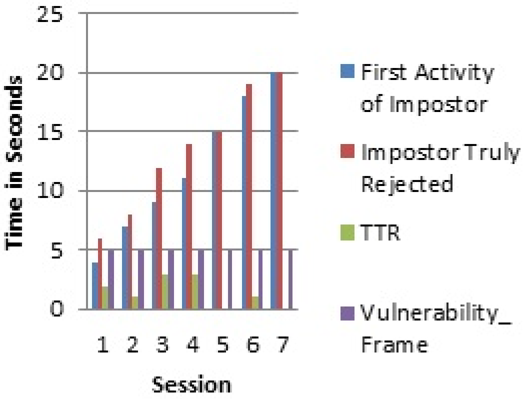


Fig. 7. Plot of *TTR* in Different Sessions.

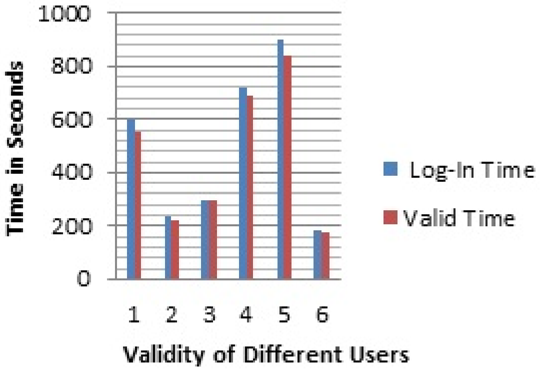


Fig. 8. Plot of Validity for Different Users.

Figure 7 represents *TTR* metric in different sessions of a user. Here, *vulnerability-frame* is set to 5 seconds. It is seen from the figure that, *TTR* in different sessions are less than *vulnerability-frame*, which ensures integrity of the proposed authentication mechanism in remote health monitor system. Figure 8 represents high validity of different users by using proposed authentication mechanism, which ensures high accuracy. It means most of the log-in session of a valid user is effectively utilized by that user. In Figure 9, *PTTR* is plotted against validity, which represents *VAAC*. Area under *VAAC* represents overall performance of proposed semi-continuous authentication mechanism. This analysis part ensures that proposed fused bio-authentication mechanism shows reliable result in proposed remote health monitor framework.

5. CONCLUSION

Remote health monitoring could help patients, aged people to live safely and independently in their own homes, which will be beneficial to the society. Intelligence of remote health monitor framework

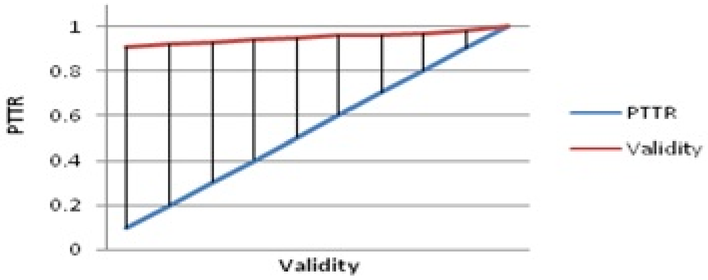


Fig. 9. Plot of *PTTR* vs. Validity in Validity Acceptability Characteristic Curve (*VACC*).

may lead to major catastrophe without proper security consideration. Most of the researches in the related field are still in their infancy. In this paper, a framework is proposed to identify authentic end-users (healthcare experts) accurately. Trust based multi-factor bio-authentication (semi-continuous) mechanism is proposed here by fusing keystroke analysis with face recognition to enhance reliability of authentication technique and reduce probability of intrusion at remote health monitor framework. At present, work is on to implement and analyzes novel authentication mechanism of the proposed framework in detail.

BIBLIOGRAPHY

[1] AHMED A. A., TRAORE, I., Biometric Recognition Based on Free-Text Keystroke Dynamics, IEEE Transactions on Cybernetics, 2014, Vol. 44, No. 4, pp. 458-472.

[2] BHATTASALI T., SAEED K.,Two Factor Remote Authentication in Healthcare, In: Proceedings of IEEE International Workshop on Internet of Smart objects: Computing, Communication and Management (CCMIoS), 2014, to be uploaded in IEEE Xplore.

[3] BHATTASALI T., CHAKI R., CHAKI N.,Secure and Trusted Cloud of Things, In: Proceedings of India Conference, INDICON 2013, IEEE Xplore, 2013, pp. 1-6.

[4] BHATTASALI T., CHAKI R., CHAKI N.,Study of Security Issues in Pervasive Environment of Next Generation Internet of Things, In: Proceedings of CISIM 2013, Springer, LNCS, 2013, pp. 206-217.

[5] HIPAA Security Guidance, Department of Health and Human Services, USA, Available online at: http://www.hhs.gov/ ocr/privacy/ hipaa/ administrative/securityrule/remoteuse.pdf.

[6] HL7 Version 3 Standard: Privacy, Access and Security Services (PASS) - Access Control, Release 1, V3, PaaS, Available online at: http://www.hl7.org/ implement/standards/product-brief.cfm?product-id=73

[7] KAVITHA S. V., A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, Elsevier, 2011, Vol. 34, No. 1, pp. 1-11.

[8] LAKSHMIPRABHA N. S., BHATTACHARYA J., MAJUMDER S., Face recognition using multimodal biometric features, In: Proceedings of International Conference on Image Information Processing (ICIIP), 2011, pp. 1-6.

[9] MEINGAST M., ROOSTA T., SASTRY S., Security and Privacy Issues with Healthcare Information Technology, In: Proceedings of IEEE EMBS Annual International Conference, 2006, pp. 5453-5458.

[10] MISHRA A., Multimodal Biometrics it is: Need for Future Systems, International Journal of Computer Applications, 2010, Vol. 3, No. 4, pp. 28-33.

[11] RYBNIK M., TABEDZKI M., ADAMSKI M., SAEED K., An Exploration of Keystroke Dynamics Authentication using Non-fixed Text of Various Length, In: Proceedings of International Conference on Biometrics and Kansei Engineering, 2013, pp. 245-250.

[12] SAMARIA F., HARTER A., Parameterisation of a stochastic model for human face identification, In: Proceedings of IEEE Workshop on applications of computer vision, 1994, pp. 138-142.

[13] VENKATASUBRAMANIAM K. K., GUPTA S. K. S., Security for Pervasive Health Monitoring Sensor Applications, In: Proceedings of International Conference on Intelligent Sensing and Information Processing (ICPSIP), 2006, pp. 197-202.

[14] YAZDANPANAH A. P., FAEZ K., AMIRFATTAHI R., Multimodal biometric system using face, ear and gait biometrics, In: Proceedings of International Conference on Information Sciences Signal Processing and their Applications (ISSPA), 2010, pp. 251 - 254.