A New Multilevel Hierarchial Architecture Approach for Secure User Authentication and Session Management

Akshatha B M, Harshini B H
Kavya S B, Kavya M S
B.E. VIII sem, Dept. of CS&E,
Kalpataru Institute of Technology,
Tiptur, Karnataka

Sanjay Kumar N V
Assoc. Prof. ,Dept. of CS&E,
Kalpataru Institute of Technology,
Tiptur, Karnataka

***Abstract*- The strong need for user-friendly systems that can secure our assets and protect our privacy without losing our identity in this digital world is most obvious. Session management in distributed internet services is traditionally based on username and password and most of the computer vision based applications provide security through biometrics. The mechanisms of user session expiration using classic timeouts and the identity of a user is considered immutable during the entire session. This paper explores promising alternatives offered by applying a new approach for user verification and session management by a secure protocol. The context aware security by multilevel architecture (CASHMA) is applied for adaptive timeouts based on the quality, frequency and type of secure biometric authentication on the internet. The functional behavior of the protocol is illustrated using model based quantitative analysis to assess the ability of the protocol to contrast security attacks by different kinds of attackers.**

1 INTRODUCTION

In relatively every part of human life have figuring gadgets, (for example, PC, advanced cell, tablet, or shrewd watches) wind up essential devices. The correspondence administrations, flight and monetary administrations are particularly controlled by PC frameworks. Individuals depend with crucial data such as therapeutic and criminal records, oversee exchanges, pay bills also, private archives. In any case, this expanding reliance on PC frameworks, combined with a developing accentuation on worldwide openness in the internet, has disclosed new dangers to PC framework security. Also, violations and shams in the internet are all over the place. For most existing PC frameworks, once the client's personality is checked at login, the framework assets are accessible to that client until he/she leaves the framework or on the other hand bolts the session. Actually, the framework assets are accessible to any client amid that period. This might be proper for low security situations, however can prompt session capturing, in which an aggressor focuses on an open session, e.g. whenever individuals leave the PC unattended for shorter or longer periods when it is opened, for instance to get some espresso, to go furthermore, converse with a partner, or just in light of the fact that they don't have the propensity for locking a PC in light of the burden. In high hazard conditions or where the cost of unapproved utilize of a PC is high.

By utilizing nonstop check the character of the human working the PC is persistently checked. Username and secret word of conventional validation framework is get supplant by biometric characteristic if there should be an occurrence of biometric system. Biometrics are the science and innovation of deciding and recognizing the amend client personality in view of physiological and behavioral characteristics which incorporates confront acknowledgment, retinal outputs, unique mark voice acknowledgment and keystroke flow. Biometric client confirmation is planned as a solitary shot check .Single shot check gives client confirmation just at the login time. On the off chance that the personality of client is checked once, at that point assets of the framework are accessible to client for settled timeframe and the personality of client is perpetual for entire session. An essential arrangement is to utilize short session timeouts and intermittently ask for the client to enter his/her qualifications over and over.

To opportune recognize abuses of PC assets and keep that an unapproved client perniciously replaces an approved one, arrangements in light of multi-modular bio-metric persistent confirmation are proposed, transforming client check into a persistent process instead of onetime event. To stay away from that a solitary biometric quality is fashioned, biometrics confirmation can depend on numerous biometrics characteristics .new approach for clients check and session administration are examined in this paper is characterized and actualized in the setting of the multi-modular biometric validation framework CASHMA-(Setting Mindful Security by Progressive Multilevel Engineering). The CASHMA framework understands a secure biometric validation benefit on the Web, in this clients need to recall just a single username and utilize their biometric information instead of passwords to verify in various web administrations. CASHMA work safely with any sort of web benefit for instance web based saving money, military zones, and air terminal zone which require high security administrations.

2 PRELIMINARIES

2.1 Continuous Authentication

A critical issue that consistent validation points to handle is the likelihood that the client gadget (table, PC, and so on.) is utilized, stolen or persuasively taken after the client has just signed into a security-basic administration, or that the correspondence channels or the biometric sensors are hacked.

In [7] a multi-modular biometric check framework is composed and created to recognize the physical nearness of the client signed in a PC. The proposed approach expect that first the client sign in utilizing a solid confirmation method, at that point a consistent check process is begun in light of multi-modular biometric. Confirmation disappointment together with a preservationist gauge of the time required to subvert the PC can naturally bolt it up. Likewise, in [5] a multi-modular biometric check framework is exhibited, which ceaselessly confirms the nearness of a client working with a PC. On the off chance that the check comes up short, the framework responds by locking the PC and by deferring or solidifying the client's procedures.

The work in [8] proposes a multi-modular biometric constant confirmation answer for nearby access to high-security frameworks as ATMs, where the crude information procured are weighted in the client check process, in light of I) kind of the biometric qualities and ii) time, since various sensors are ready to furnish crude information with various timings. Point ii) presents the need of a transient incorporation technique which relies upon the accessibility of past perceptions: in view of the suspicion that over the long haul, the trust in the obtained (maturing) values diminishes. The paper applies a decline work that measures the vulnerability of the score processed by the check work. In [22], notwithstanding the emphasis isn't on ceaseless validation, a programmed tuning of choice parameters (limits) for successive multi-biometric score combination is exhibited: the rule to accomplish multimodality is to consider monomodal biometric subsystems successively. In [3] a wearable confirmation gadget (a wristband) is exhibited for a constant client verification and straightforward login strategy in applications where clients are roaming. By wearing the confirmation gadget, the client can login straightforwardly through a remote channel, and can transmit the confirmation information to PCs essentially moving toward them. CASHMA can work safely with any sort of web benefit, incorporating administrations with high security requests as web based managing an account administrations.

Another approach for client confirmation and session administration that is connected in the setting mindful security by various leveled multilevel models (CASHMA) [1]) framework for secure biometric verification on the Internet.. Contingent upon the inclinations and requirements of the proprietor of the web benefit, the CASHMA verification administration can supplement a customary authentication benefit, or can supplant it.

The approach we presented in CASHMA for usable and very secure client sessions is a consistent consecutive (a solitary biometric methodology on the double is displayed to the framework [22]) multi-modular biometric confirmation convention, which adap-tively processes and revives session timeouts based on the put stock in put in the customer. Such worldwide trust is assessed as a numeric esteem, figured by persistently assessing the put stock in both in the client and the (biometric) subsystems utilized for getting biometric information. In the CASHMA setting, every subsystem contains all the equipment/programming components important to procure and confirm the genuineness of one bio-metric characteristic, including sensors, correlation calculations and every one of the offices for information transmission and administration. Trust in the client is resolved based on recurrence of updates of new biometric tests, while confide in each sub-framework is figured based on the quality and assortment of sensors utilized for the securing of biometric tests, and on the danger of the subsystem to be interfered.

2.2 Quantitative Securtiy Evaluation

Security appraisal depended for quite a while on subjective examinations as it were. Leaving aside exploratory assessment and information examination [26], [25], demonstrate based quantitative security evaluation is still a long way from being a built up strategy regardless of being a dynamic research zone. Particular formalisms for security assessment have been presented in writing, empowering to some degree the measurement of security. Assault trees are firmly identified with blame trees: they consider a security rupture as a framework failure and depict sets of occasions that can prompt framework disappointment in a combinatorial way [14]; they however don't consider the idea of time. Assault diagrams [13] expand assault trees by presenting the idea of state, along these lines permitting more intricate relations between assaults to be portrayed. Mission situated hazard and plan investigation (MORDA) surveys framework chance by computing assault scores for an arrangement of framework assaults. The scores depend on foe assault inclinations and the effect of the assault on the framework [23]. The as of late presented Foe VIew Security Evaluation formalism [12] broadens the assault diagram idea with quantitative data what's more, bolsters the meaning of various assailants profiles.

2.3 Basic Defination

In this area we present the fundamental definitions that are received in this paper. Given n unimodal biometric. The CASHMA validation benefit incorporates: I) an confirmation server, which communicates with the customers, ii) a set of high-performing computational servers that perform correlations of biometric information for confirmation of the enlisted clients, and iii) databases of layouts that contain the biometric layouts of the enlisted clients (these are required for client confirmation/check). The web administrations are the different administrations that utilization the CASHMA validation benefit and request

the confirmation of enlisted clients to the CASHMA confirmation server. These administrations are possibly any sort of Internet administration or application with necessities on client legitimacy. They must be enlisted to the CASHMA verification benefit, communicating likewise their confide in edge.

The constant verification convention investigated in this paper is autonomous from the chosen building decisions also, can work without any distinctions if formats and highlight sets are utilized as opposed to transmitting crude information, or autonomously from the arrangement of received counter measures.

3 THE CASHMA ARCHITECTURE

CASHMA implies Context-Aware Security by Hierarchical Multilevel Architectures. This framework is utilized for secure biometric validation on the web. CASHMA can work safely with any sort of web benefit, including administrations with high security requests as web based managing an account administrations. The CASHMA verification benefit supplant the conventional validation benefit.

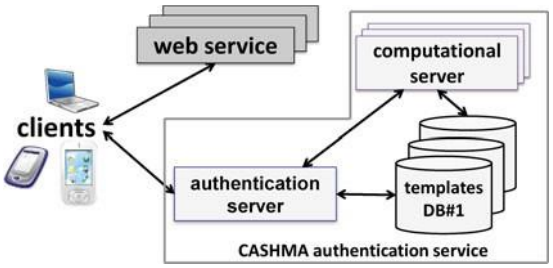

Fig.1. Overall view of the CASHMA architecture

The framework design is comprising of the CASHMA verification benefit, the customers and the web administrations and they are associated through correspondence channels. Fig. 1 portrays the consistent verification framework to a web benefit. The validation server, which interfaces with the customers, computational servers that perform examinations of biometric information for check of the clients, and databases of formats contains the biometric layouts of the clients (that are required for client validation or confirmation reason). The web benefit requests the validation of clients to the CASHMA validation server. These administrations are any sort of Internet benefit. At last, by customers we mean the clients' gadgets like (PCs, Desktop PCs, tablets, and so forth.) which gain the biometric information relating to the different biometric attributes from the clients, and transmit those information to the CASHMA validation server towards an objective web benefit. A customer contains. I) Sensors - get the crude information, ii) the CASHMA application - transmits the crude information to the verification server. The CASHMA verification server applies client confirmation and check methodology that analyze the crude information with the biometric layouts put away.

Consider web based keeping money where a client needs to sign into an internet saving money benefit utilizing an advanced mobile phone. Here client and web administrations must be enlisted to CASHMA confirmation benefit also, client must be introduced CASHMA application on his savvy telephone. The cell phone contacts the web based saving money benefit, which answers asking for the customer to contact the CASHMA validation server and get a confirmation testament. Utilizing the CASHMA application, the cell phone sends its extraordinary identifier and biometric information to the verification server for check. The verification server checks the client character, and gives the entrance on the off chance that: I) it is enlisted in the CASHMA validation benefit, ii) it has rights to get to the internet managing an account administration and, iii) the gained biometric information coordinate those put away in the layouts database related to the given identifier. If there should arise an occurrence of effective client check, the CASHMA confirmation server discharges a verification endorsement to the customer, demonstrating its personality to outsiders, and incorporates a timeout that sets the most extreme span of the client session. The customer introduces this endorsement to the web benefit, which confirms it and stipends access to the customer. The CASHMA application works to ceaselessly keep up the session open: it straightforwardly obtains biometric information from the client, and sends them to the CASHMA validation server to get another endorsement.
Such authentication, which incorporates another timeout, is sent to the web administration to additionally broaden the client session.

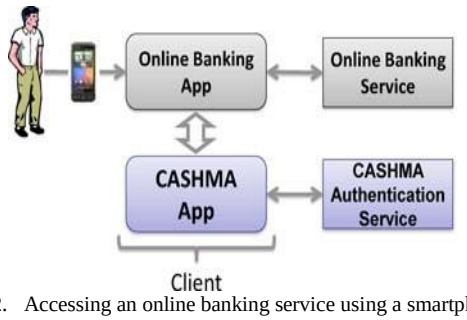

Fig.2. Accessing an online banking service using a smartphone

4 THE CASHMA CERTIFICATE

The data contained in the body of the CASHMA testament transmitted to the client by utilizing the CASHMA confirmation server, basic to perceive imperative focuses of the convention. The CASHMA endorsements comprise of Time stamp and succession number univocally recognize each testament, and it take care of from replay assaults. Id is the individual id, e.g., a number. Decision speaks to the last consequence of the check process did on the server side. It incorporates the lapse time of the session, progressively relegated by the CASHMA confirmation server. Regularly, the worldwide confide in arrange and the session timeout are consistently processed by method for considering the time prompt in which the CASHMA application secures the biometric information, to confine potential issues concerning obscure

deferrals in discussion and calculation. Because of the reality such postponements won't be predicable in earlier, essentially providing a relative timeout incentive to the client won't be reasonable, so the CASHMA server accordingly gives the supreme prompt of time at which the session must terminate. The CASHMA authentications will most likely be terminated when the lapse timeout accomplish zero.

5 THE CONTINUOUS AUTHENTICATION PROTOCOL

The nonstop validation convention permits giving versatile session timeouts to a web administration to set up and keep up a safe session with a customer. The timeout is adjusted based on the assume that the CASHMA validation framework puts in the biometric subsystems and in the client. The execution of the convention is made out of two back to back stages: the underlying stage and the support stage. The underlying stage intends to confirm the client into the framework and build up the session with the web benefit. Amid the upkeep stage, the session timeout is adaptively refreshed when client personality check is performed utilizing new crude information gave by the customer to the CASHMA confirmation server. The client (the customer) contacts the web benefit for an administration ask for; the web benefit answers that a substantial testament from the CASHMA validation n benefit is required for confirmation.

A. Initial Phase:

Utilizing the CASHMA application, the customer contacts the CASHMA validation server. The initial step comprises in obtaining and sending at time t0 the information for the extraordinary biometric qualities, particularly chose to play out a solid confirmation strategy (stage 1). The application expressly shows to the client the biometric qualities to be given and conceivable retries. The CASHMA confirmation server dissects the biometric information got and plays out a confirmation methodology. Two distinct potential outcomes emerge here. In the event that the client character isn't checked (the worldwide trust level is underneath the trust limit gmin), new or extra biometric information are asked (back to stage 1) until the base trust limit gmin is come to. Rather if the client character is effectively confirmed, the CASHMA confirmation server verifies the client, processes an underlying timeout of length T0 for the client session, set the lapse time at T0 + t0, makes the CASHMA authentication and sends it to the customer (stage 2). The customer advances the CASHMA authentication to the web benefit (stage 3) coupling it with its demand. The web benefit peruses the testament and approves the customer to utilize the asked for benefit (stage 4) until time t0 +T0.

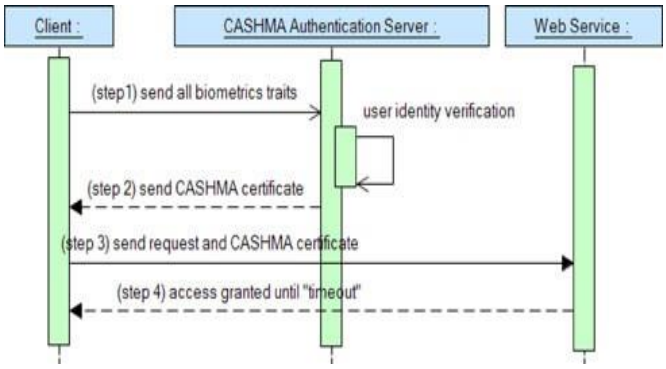

Fig.3. Initial phase in case of successful user authentication.

B. Maintenance Phase:

At the point when some time the client programming get crisp (new) crude information (comparing to one biometric attribute), it imparts them to the CASHMA confirmation server [3] (stage 5). The biometric information can likewise be purchased straightforwardly to the client; The CASHMA verification server gets the biometric information from the client and confirms the personality of the individual. In the event that confirmation shouldn't be triumphant, at that point the client is set apart as not proficient, and in this manner the CASHMA verification server does not perform. In the event that confirmation is fruitful, the CASHMA validation server applies the calculation to adaptively appraise a pristine timeout of period Ti , the lapse time of the session at time Ti+ ti and afterward it makes and sends another testament to the customer. The client gets another declaration and advances it to the web benefit; the online administration peruses the authentications and sets the session timeout to lapse at time ti+ Ti. For lucidness, stages 1-4 are spoken to in Fig. 4for the case of positive client check best [1]. Support stage [1]. It is made out of three stages rehashed iteratively: When at time ti the customer application secures later (new) crude information (comparing to one biometric quality), it imparts them to the CASHMA confirmation server (stage 5). The biometric information can likewise be gotten straightforwardly to the client; the client may all things considered settle on a choice to give biometric information which are impossible purchased in a conspicuous approach (e.g., unique finger impression). At last when the session timeout goes to lapse, the customer could unequivocally tell to the client that new biometric information are wanted.

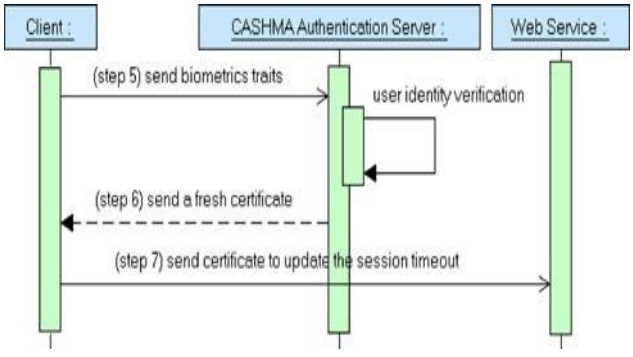

Fig.4. Maintenance phase in case of successful user verification

The CASHMA verification server gets the biometric information from the client and confirms the ID of the customer. On the off chance that confirmation shouldn't be fruitful, the customer is set apart as not genuine, and accordingly the CASHMA verification server does not capacity to invigorate the session timeout. This doesn't show that the client is cutoff from the present session: if other biometric information are given sooner than the timeout lapses, it is in any case possible to get another declaration and invigorate the timeout. On the off chance that check is fruitful, the CASHMA validation server applies the algorithm[1] to adaptively figure a pristine timeout of length Ti , the termination time of the session at time Ti+ ti and after that it makes and sends a pristine authentication to the buyer (stage 6). The customer gets the accreditation and supplies it to the online supplier; the web transporter reads the authentications.

C. *Trust Levels And Timeout Computation*

In this segment the fundamental definitions are present that are embraced in this paper. Given a unimodal biometric subsystem Sk with k = 1, 2,..,n that can choosing conditionally on the realness of a client, the False Non-Match Rate, FNMRk, is the extent of real examinations which result in false which does not matches. False non-coordinate is the choice of non-coordinate when looking at biometric tests which are in the type of same biometric source. The likelihood the unimodal framework Sk wrongly rejects a substantial client. Oppositely, the False Match Rate, FMRk, is the likelihood that the unimodal subsystem Sk makes a false match mistake, it wrongly chooses that an invalid client is as opposed to legitimate one. A false coordinate mistake in a unimodal framework would prompt confirm invalid client. To make simple the dialog yet by not losing the general materialness of the approach, we assume that each sensor permits just a single biometric quality.

1) Trust Levels and Timeout Computation

The calculation to express the termination time of the session that executes iteratively on the CASHMA confirmation server it takes another timeout and similarly the termination time each time the CASHMA verification server gets new biometric information from a client. Give us a chance to think about that the underlying stage occurs at time $t0$ when biometric information is gained and transmitted by the CASHMA utilization of the client and that amid the upkeep stage at time ti> t0 for any i=1,…m. new biometric information is gained by the CASHMA use of the client. The means of the calculation depicted from this point forward are executed .To facilitate the comprehensibility of the documentation, in the accompanying the client u is frequently precluded.

2) Computation of Trust in the Subsystems

The calculation begins registering the trust in the subsystems .Intuitively, the subsystem trust level could be just set to the static esteem m(Sk,t)=1 - FMR(Sk).for each unimodal subsystem Sk and whenever t (we expect that data on the subsystems utilized, including their FMRs, is contain edam a vault open by the CASHMA validation server). Rather we apply a punishment capacity to align the trust in the subsystems based on its use. Essentially, in our approach the more the subsystem is utilized, the less it is trusted: to dodge that a malevolent client is required to control just a single biometric characteristic (e.g., through sensor caricaturing) to keep validated to the online administration, we diminish the trust in those subsystems which are more than once used to get the biometric information.

5 SECURITY EVALUATION

A total investigation of the CASHMA framework was completed amid the CASHMA venture [1], supplementing tradi-tional security examination strategies with systems for quantitative security assessment. Subjective security analy-sister, having the goal to recognize dangers to CASHMA and select countermeasures, was guided by general and acknowledged mappings of biometric assaults and assault focuses as [9], [10], [11], [21]. A quantitative security examination of the entire CASHMA framework was likewise performed [6]. As this paper centers around the nonstop confirmation convention as opposed to the CASHMA engineering, we quickly summa-rize the fundamental dangers to the framework distinguished inside the task (Section 6.1), while whatever remains of this area (Sec-tion 6.2) centers around the quantitative security evaluation of the consistent verification convention.

6 IMPLEMENTATION

The usage of the CASHMA model incorporates confront, voice, iris, unique mark and online dynamic written by hand signature as biometric attributes for biometric booths and PCs/workstations, depending on-board gadgets when accessible or pluggable adornments if necessary. On cell phones just face and voice acknowledgment are connected: iris acknowledgment was dis-checked because of the challenges in getting top notch iris filters utilizing the camera of business gadgets, and manually written mark acknowledgment is illogical on a large portion of cell phones today accessible on showcase (bigger presentations are required). At long last, unique finger impression acknowledgment was disposed of in light of the fact that few cell phones incorporate a unique finger impression peruser. The chose biometric characteristics (face and voice) suit the should be procured straightforwardly for the constant verification convention portrayed.

A model of the CASHMA engineering is as of now accessible, giving portable parts to get to a secured web-application. The customer depends on the Adobe Flash [19] innovation: it is a particular customer, written in Adobe Actions Script 3, ready to access and control the on-board gadgets keeping in mind the end goal to get the crude information required for biometric authentication. If there should arise an occurrence of cell phones, the CASHMA customer component is acknowledged as a local Android application (utilizing the Android SDK API 12). Tests were directed on advanced cells Samsung Galaxy S II, HTC Desire, HTC Desire HD and HTC Sensation with OS Android 4.0.x. By and large from the executed tests, for the

cell phones considered we accomplished FMR ¼ 2.58% for confront acknowledgment and FMR ¼ 10% for voice. The measurements of biometric information obtained utilizing the considered cell phones and traded are approximately 500 KB. Not surprisingly from such restricted measurement of the information, the obtaining, pressure and transmission of these information utilizing the said cell phones did not raise issues on execution or correspondence data transmission. Specifically, the time required to build up a protected session and transmit the biometric information was considered adequately short to not trade off ease of use of the cell phone. With respect to confirmation benefit, it keeps running on Apache Tomcat 6 servers and postgres 8.4 databases.

The web services are, rather, acknowledged utilizing the Jersey library (i.e., a JAX-RS/JSR311 Reference Implementation) for building restful web administrations. At long last, the illustration application is a custom gateway developed as a Rich Internet Application utilizing Sencha ExtJS 4 JavaScript structure, incorporating distinctive outer online administrations (e.g., Gmail, Youtube, Twitter, Flickr) made accessible progressively following the present trust estimation of the continuous confirmation convention.

7 CONCLUSION

Session administration framework is completely in light of username what's more, secret key, and sessions are ended by express logouts or on the other hand by the lapse of session timeouts. Strategies utilized for persistent validation utilizing distinctive biometrics. Beginning one time login check is deficient to address the hazard associated with post signed in session. We abused the novel probability acquainted by biometrics with characterize a convention for nonstop validation that enhances security and convenience of client session. The convention processes versatile timeouts on the premise of the confide in postured in the client movement and in the quality and sort of biometric information procured straightforwardly through checking in foundation the client's activities. Constant validation check with multi - modular biometrics enhances security and ease of use of client session. The capacities proposed for the assessment of the session timeout are chosen among an extensive arrangement of conceivable options.

We misused the novel plausibility acquainted by biometrics with characterize a convention for nonstop validation that enhances security and ease of use of client session. The proto-col registers versatile timeouts based on the put stock in postured in the client action and in the quality and sort of bio-metric information gained straightforwardly through checking in foundation the client's activities.

Some building outline choices of CASHMA are here talked about. In the first place, the framework trades crude information and not the highlights extricated from them or layouts, while cripto-token methodologies are not considered; as bantered in Section 3.1, this is because of engineering choices where the customer is kept extremely basic. We comment that our proposed convention works without any progressions utilizing highlights, layouts or crude information. Second, protection concerns ought to be tended to thinking about National enactments. At display, our model just plays out a few keeps an eye on confront acknowledgment, where just a single face (the greatest one rusting from the face detection phase specifically on the customer gadget) is considered for character check and the others erased. Third, when information is gained in an uncontrolled situation, the nature of bio-metric information could unequivocally rely upon the environment. While playing out a customer side quality examination of the information gained would be a sensible way to deal with lessen computational load on the server, and it is good with our target of planning a convention free from quality evaluations of pictures (we simply consider a sensor believe), this conflicts with the CASHMA necessity of having a light client.

REFERENCES

[1] CASHMA-Context Aware Security by Hierarchical Multilevel Architectures, MIUR FIRB, 2005.
[2] Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini, Angelo Marguglio, Andrea Bondavalli ”Continuous and Transparent User Identity Verification for Secure Internet Services” IEEE Transaction on De-pendable and Secure Computing, VOL. 12,NO. 3,JUNE 2015.
[3] Anil K. Jain, Sharath Pankanti, Salil Prabhakar, Lin Hong, Arun Ross, James L. Wayman, ”Biometrics: A Grand Challenge” International Conference on Pattern Recognition , Aug 2004.
[4] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, “ContinuousVerification Using Multimodal Biometrics,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 687-700, Apr. 2007.
[5] T.F. Dapp, “Growing Need for Security in Online Banking: Biometrics Enjoy Remarkable Degree of Acceptance,,” Banking & Technology Snapshot, DB Research, Feb. 2012.
[6] A. Ceccarelli, A. Bondavalli, F. Brancati, and E. La Mattina,“Improving Security of Internet Services through Continuous and Transparent User Identity Verification,” Proc. Int’l Symp. Reliable Distributed Systems (SRDS), pp. 201-206, Oct. 2012.
[7] L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina,“Quantitative Security Evaluation of a Multi-Biometric Authentication System,” Proc. Int’l Conf. Computer Safety, Reliability and Security, pp. 209-221, 2012.
[8] L. Hong, A. Jain, and S. Pankanti, “Can Multibiometrics Improve Performance?” Proc. Workshop on Automatic Identification AdvancesTechnologies (AutoID ’99) Summit, pp. 59-64, 1999.
[9] S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, “Using Continuous Biometric Verification to Protect Interactive Login Sessions,” Proc. 21st Ann. Computer Security Applications Conf. (ACSAC ’05), pp. 441-450, 2005.
[10] Biometric System Base Secure Authentication Service for Session Management Nilima Deore, Prof. C.R.Barde International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 12, December 2015.
[11] A. Ceccarelli, A. Bondavalli, F. Brancati, and E. La Mattina, “Improving Security of Internet Services through Continuous and Transparent User Identity Verification,” Proc. Int’l Symp. Reliable Distributed Systems (SRDS), pp. 201-206, Oct. 2012.
[12] Adobe Products List, http://www.adobe.com/products, 2014.
[13] T.F. Dapp, “Growing Need for Security in Online Banking: Bio- metrics Enjoy Remarkable Degree of Acceptance,,” Banking & Technology Snapshot, DB Research, Feb. 2012.
[14] A.K. Jain, A. Ross, and S. Pankanti, “Biometrics: A Tool for Infor- mation Security,” IEEE Trans. Information Forensics and Security, vol. 1, no. 2, pp. 125-143, June 2006.