ELSEVIER

Scopus

doi

Journal of Vibration Engineering

ISSN:1004-4523

Registered

- SCOPUS
- GOOGLE SCHOLAR
- DIGITAL OBJECT IDENTIFIER (DOI)
- IMPACT FACTOR 6.1

Our Website
www.jove.science

Multi-ModalUserAuthenticationTechniqueusingKeystroke,MouseandGameDynamics:An Effectiveand SecureApproach

Sindhu.B
Research ScholarDepartmentofComputerScienceand EngineeringAdikavi NannayaUniversity AndhraPradesh,India.
ORCIDID:0000-0001-6543-2777

Dr.KeziaRani.B
Assistant ProfessorDepartmentofComputerScienceand EngineeringAdikavi NannayaUniversity AndhraPradesh,India.
ORCIDID:0000-0002-4162-0148

ABSTRACT

Robust user authentication is important to ensure that only authorized personnel gainaccess to sensitive data or resources, thereby preventing potential security breaches. Thisproposalpresentsanoveluserauthenticationsystemthatcombinesthreedifferentbiometricmodalities: Keystroke dynamics, Mouse dynamics, and Game behaviour dynamics. Thesystemaimstoimprovethesecurityofuserauthenticationbyleveragingtheuniquecharacteristics of these modalities. Keystroke dynamics involve analyzing the way a usertypes on a keyboard. Mouse dynamics analyze the way a user moves their mouse. Gamebehaviourdynamicsanalyzethewayauserplaysagame.WithMulti-modalbiometrics,theproposedauthenticationsystemcancreateamorecomprehensiveandaccurateprofileoftheuser'sbehaviour,makingitimpossibleforunauthorizeduserstogainaccess.Thesystemusesstatisticalalgorithmstoanalyzethedatacollectedfromeachmodalityandgeneratesauniquescore for each user, which is then compared against the user's stored profile to determine iftheyareauthenticated.

Keywords:

Biometrics,Multi-modalBiometrics,Robustuserauthentication,Keystrokedynamics,Mousedynamics,andGamebehaviourdynamics.

INTRODUCTION

Biometrics refers to the measurement and analysis of unique physical or behavioralcharacteristics of individuals to verify their identity. Biometric technologies use the mostunique characteristics of individuals to accurately identify them for access control, security,orotherpurposes.Biometrictechnologyoffersahighlyaccurateandreliablewayofauthentication, and has become increasingly popular in recent years as a more secure andconvenientalternativetotraditionalauthenticationmethods[1].

Biometrics is widely used in the field of user authentication, particularly insettingswheresecurityandaccesscontrolarecritical.Biometricauthenticationistheprocessofverifyinganindividual'sidentitybyanalyzingtheiruniquephysicalorbehavioralcharacteristics[2].

Biometric authentication offers several advantages over traditional authenticationmethods,suchaspasswordsandPINs,asitprovidesamoresecureandconvenientwayto

verifyanindividual'sidentity.Biometricauthenticationalsoeliminatestheneedtorememberand enter passwords, which can be forgotten or stolen, leading to increased security risks[3,4].

In addition to traditional authentication methods, biometric authentication is alsoincreasingly used in mobile devices, such as smartphones and tablets, as well as in financialtransactions, healthcare, and border control. While biometric authentication offers manybenefits,italsoraisesconcernsaboutprivacy,datasecurity,andpotentialmisuseofpersonali nformation,whichmustbecarefullyaddressedtoensuretheresponsibleuseofthistechnology[5].

ClassificationofBiometrics

Biometrics are generally classified into two categories: physiological biometrics andbehavioralbiometrics.

1. Physiologicalbiometrics:Thesearebasedonphysicalcharacteristicsofthebody,suchasfinger prints,irispatterns,facialfeatures,handgeometry,andDNA.Thesebiometricsareconsidered highly unique and difficult to forge, as they are based on features that aredeterminedbygeneticsorotherphysicalfactors.

2. Behavioral biometrics: These are based on patterns of behavior or actions, such askeystroke dynamics, gait analysis, signature dynamics, and voice recognition. Thesebiometricsareconsideredlessuniquethanphysiologicalbiometrics,butcanstillprovide ahighlyaccuratewayofidentifyingindividualsbasedontheirbehaviorpatterns.

Bothphysiologicalandbehavioralbiometricshavetheirownadvantagesanddisadvantage s,andthechoiceofwhichbiometrictousewilldependonthespecificapplicationandthelevelofsecu rityrequired.Insomecases,acombinationofbothphysiological and behavioral biometrics may be used to provide a more secure and accurateauthenticationsystem[6].

Physiological biometrics are based on physical characteristics of the body, such asfingerprints,irispatterns,facialfeatures,handgeometry,andDNA.Herearesomecommontype sofphysiologicalbiometrics:

- Fingerprintrecognition:Thisisthemostwidelyusedbiometrictechnologyandinvolvesanalyz ingtheuniquepatternsofridgesandvalleysonanindividual'sfingers.

- Facial recognition: This involves analyzing facial features, such as the distance betweentheeyes,theshapeofthenose,andthecontoursofthejawline.

- Irisrecognition:Thisinvolvesanalyzingtheuniquepatternsoftheiris,thecoloredpartoftheeye .

- Handgeometry:Thisinvolvesanalyzingthesize,shape,andproportionsofanindividual'shand ,includingthelengthoffingersandthedistancebetweenjoints.

- DNA analysis: This involves analyzing an individual's genetic code to identify uniquepatternsthatcanbeused foridentification.

- Retinarecognition:Thisinvolvesanalyzingtheuniquepatternsofthebloodvesselsinthebacko ftheeye.

- Voicerecognition:Thisinvolvesanalyzinganindividual'svoice,includingpitch,tone,andaccent.

Behavioralbiometricsarebasedonpatternsofbehaviororactions.Commontypesofbehavioralbiometrics are:

- Keystrokedynamics:Thisinvolvesanalyzingtheuniquepatternsofanindividual'stypingbehavior,suchasthespeedandrhythmoftheirkeystrokes.
- Gaitanalysis:Thisinvolvesanalyzingtheuniquewayanindividualwalks,includingtheirstridelength,posture,andotherwalkingcharacteristics.
- Signaturedynamics:Thisinvolvesanalyzingtheuniquepatternsofanindividual'ssignature,includingthepressure,speed,anddirectionoftheirpenstrokes.
- Voicerecognition:Thisinvolvesanalyzinganindividual'svoice,includingpitch,tone,andaccent.
- Mousedynamics:Thisinvolvesanalyzingtheuniquepatternsofanindividual'smousemovements,suchastheirspeedandrhythm.
- Cognitivebiometrics:Thisinvolvesanalyzinganindividual'scognitivebehavior,suchastheirresponsetimeanddecision-makingpatterns[7-15].

ApplicationsofBiometrics

Biometricshasawiderangeofapplicationsacrossvariousindustriesandsectors.Someofthecommonapplicationsofbiometricsare:

- PhysicalAccessControl
- TimeandAttendanceManagement
- BorderControlandLawEnforcement
- FinancialTransactions
- Healthcare
- Education

AdvantagesanddisadvantagesofBiometrics

Advantagesofbiometrics:

- Highaccuracy
- Security
- Convenience
- Speed
- Non-transferable

Disadvantagesofbiometrics:

- Cost
- Privacyconcerns
- Limitedscalability
- Inaccuracy
- Vulnerabletospoofing[4]

1. LITERATUREREVIEW

Keystrokedynamics

Keystrokedynamics,alsoknownaskeystrokebiometricsortypingdynamics,isabehavioralbiometric modality that involves analyzing the unique pattern of typing behavior of anindividual. This modality captures various features such as key hold time, key release time,keypressforce,andtypingrhythm.Keystrokedynamicshasbeenstudiedextensivelyfor

over two decades and has shown promising results in various applications, including userauthentication,computeraccesscontrol,andidentityverification.

Recentremarkableworksinkeystrokedynamicswasby Monroseetal.(2000),whodemonstrated the feasibility of using keystroke dynamics as a biometric for authentication.They collected keystroke data from a group of users typing a predefined text and evaluatedthe system's performance based on false acceptance rate (FAR) and false rejection rate(FRR).Theyfoundthatkeystrokedynamicscanachievehighaccuracyinuserauthentication,withanaverageFARof1.03%andanaverageFRRof2.85%.

Othmanetal.(2016)proposedakeystrokedynamics-baseduserauthenticationsystemusinga hybrid feature selection technique that combines statistical and correlation-based featureselectionmethods.Theproposedsystemachievedanaccuracyof95.5%,whichishigherthantraditionaluserauthenticationmethodssuchaspasswordsandPINs.

Carmona-Duarteetal.(2021)proposedadeeplearningapproachthatcombinesaconvolutionalneuralnetwork(CNN)andarecurrentneuralnetwork(RNN)toidentifyusersbased on their keystroke dynamics. They collected keystroke data from 100 users typing apredefinedtextandachievedanaccuracyof92.6%.

Wang et al. (2020) proposed a continuous mobile user authentication system that combineskeystroke dynamics and smartphone sensor data, including accelerometer and gyroscopedata. The proposed system achieved an accuracy of 98.9%, which is higher than usingkeystrokedynamicsalone.

Keystroke dynamics is a promising behavioral biometric modality that has shown highaccuracy in user authentication and identification. Deep learning approaches and combinationwith other modalities have further improved the system's performance. However, there arestillchallengessuchasvariabilityintypingbehaviorduetofatigue,stress,anddifferentinputdevices. Future research could focus on addressing these challenges and further improvingtheaccuracyandusabilityofkeystrokedynamics-basedsystems.[22-25]

Mousedynamics

Mouse dynamics is a behavioral biometric modality that captures unique patterns of mousemovements and clicks of an individual. Mouse dynamics analyses various features such asthe speed of movement, the distance moved, the direction of movement, and the timing ofclicks.Thistechnologyhasgainedinterestinrecentyearsduetoitsapplicationsinauthentication andidentification.

Sae-Bae, T. et al., 2015, evaluated the effectiveness of mouse dynamics as a biometricmodality for authentication. The study analyzed the mouse dynamics of 50 participantsperformingasetofpredefinedtasks.Theresultsshowedthatmousedynamicscouldprovidean effective means of authentication, with a false acceptance rate of 2.4% and a falserejectionrateof4.4%.

Ahmed, M. et al., 2018, investigated the possibility of combining mouse dynamics withkeystroke dynamics to improve authentication performance. The study analyzed the mouseand keystroke dynamics of 30 participants performing a set of predefined tasks. The resultsshowedthatcombiningbothmodalitiessignificantlyimprovedtheauthenticationperformance,withafalseacceptancerateof0.05%andafalserejectionrateof0.10%.

Jain,S.etal.,2017,evaluatedtheperformanceofmousedynamicsforcontinuousauthentication in a simulated computer-based task environment. The study analyzed themouse dynamics of 30 participants performing a set of tasks over a period of three weeks.The results showed that mouse dynamics could provide an effective means of continuousauthentication,withanaverageequalerrorrateof5.5%.

Monaco, J. et al., 2019, focused on investigating the stability of mouse dynamics over time.The study analyzed the mouse dynamics of 30 participants over a period of six months. Theresults showed that mouse dynamics were relatively stable over time, with an average intra-classcorrelationcoefficientof0.90.

Overall, mouse dynamics show promise as a biometric modality for authentication andcontinuous authentication, and the combination of mouse dynamics with other modalitiescould lead to improved performance. However, further research is needed to address issuessuch as variability in mouse behavior and the impact of environmental factors on mousedynamics.[26-29]

Gamebehaviorbiometrics

Game behavior biometrics is a relatively new and emerging field that uses behavioral patternsexhibited by players during gameplay to identify and authenticate users. This biometricmodality analyzes various game-related behaviors such as game session duration, gameplaypatterns,andinteractionwiththegameenvironment.

Ullah, A. et al., 2018, investigated the effectiveness of game behavior biometrics for useridentificationandauthentication.Thestudyanalyzedthegamebehaviordataof50participants playing a video game, including features such as the average session duration,frequency of playing, and game completion time. The results showed that game behaviorbiometricscouldprovideaneffectivemeansofuseridentificationandauthentication,wit hafalseacceptancerateof1.23%andafalserejectionrateof2.6%.

Chang,K.etal.,2018,focusedonanalyzingthegameplaypatternsofplayerstodetectsignsof stress and cognitive overload. The study analyzed the game play data of 20 participantsplaying a puzzle game and used machine learning techniques to detect signs of stress andcognitiveoverload.Theresultsshowedthatgameplaypatternscouldbeusedasaneffectiveindi catorofcognitiveoverloadandstressinplayers,whichcouldbeusedtoadjustthegamedifficultylev elaccordingly.

Hajizadeh,S.etal.,2019,investigatedtheuseofgamebehaviorbiometricsforuserprofilingandper sonalizedgamingexperiences.Thestudyanalyzedthegameplaydataof30participantsplayingastr ategygameandusedclusteringtechniquestoidentifydifferentuserprofilesbasedontheirgameplay behavior.Theresultsshowedthatgamebehaviorbiometricscould be used to provide personalized gaming experiences by adjusting game difficulty,rewards,andchallengesbasedontheuserprofile.

Cretu, V. et al., 2020, focused on the use of game behavior biometrics for monitoringcognitive decline in older adults. The study analyzed the game behavior data of 50 olderadults playing a puzzle game and used machine learning techniques to detect signs ofcognitive decline. The results showed that game behavior biometrics could be used as aneffective means of monitoring cognitive decline in older adults, with an accuracy rate of82.3%.

Overall,gamebehaviorbiometricsshowspromiseasabiometricmodalityforuseridentificationandauthentication,personalizedgamingexperiences,andmonitoringcognitivedecline.However,furtherresearchisneededtoaddressissuessuchasthevariabilityofgamebehaviordataandtheimpactofexternalfactorsongamebehavior.[30-33]

CombinationofKeystrokeandMousedynamics:

The combination of keystroke and mouse dynamics is an emerging field of research in thedomain of biometric authentication. It has been observed that the behavior of the user interms of keystroke and mouse dynamics is unique, and can be used for authenticating theuser. Keystroke dynamics refers to the pattern of typing behavior of an individual, whereasmouse dynamics refer to the pattern of movement of the mouse. The combination of boththese behavioral biometrics provides higher accuracy and reliability in the authenticationprocess.Inthisliteraturereview,wepresentanoverviewoftheworksdoneinthecombinationofkeystrokeandmousedynamics.

Monroseetal.(1999)usedbothkeystrokeandmousedynamicstoauthenticatetheuser,andthe results showed that the combination of both provided higher accuracy as compared tousing either keystroke or mouse dynamics alone. In their study, they used a data set of 50usersandachievedanaccuracyof96.7%.

Shirazietal.(2011)usedkeystrokeandmousedynamicsforcontinuousauthentication.Theydevelopedasystemthatcontinuouslyauthenticatestheuserbasedontheirbehavior,andtheresultsshowedthatthecombinationofbothkeystrokeandmousedynamicsprovideshigheraccuracy as compared to using either one alone. They used a data set of 12 users andachievedanaccuracyof95%.

Sae-Baeetal.(2014)proposedakeystrokeandmousedynamics-basedauthenticationsystemthat uses machine learning algorithms. They used both keystroke and mouse dynamics totrainaclassifierthatcanauthenticatetheuser.Theyusedadatasetof30usersandachievedanaccuracyof96.7%.

Alzahranietal.(2020)proposedakeystrokeandmousedynamics-basedcontinuousauthenticationsystemfor mobiledevices.They usedamachinelearningalgorithmtoauthenticatetheuserbasedontheirbehavior,andtheresultsshowedthatthecombinationofboth keystroke and mouse dynamics provides higher accuracy as compared to using eitheronealone.Theyusedadatasetof20usersandachievedanaccuracyof97.5%.[34-37]

Thecombinationofkeystrokeandmousedynamicsprovides higheraccuracyandreliabilityin the authentication process. The works reviewed in this literature review demonstrate thatthecombinationofbothbehavioralbiometricscanbeusedforcontinuousauthentication,andcan provide higher accuracy as compared to using either one alone. Future research in thisarea can explore the use of keystroke and mouse dynamics in different contexts, such as intheauthenticationofindividualswithdisabilitiesorinhigh-securityenvironments.

CombinationofGamebehaviourandotherBiometricsmodalities

Manaretal.[20]proposedGametricsisagame-basedauthenticationsystemthatusessimplecognitivegamestocollectbehavioralbiometricdatafromusers.Thesystemincludesasetofgames designed to elicit specific behavioral traits such as reaction time, motor control, andattention span. The data collected from these games is used to build a behavioral biometricprofileoftheuserbyrecordingGameplayingdynamicsandMousedynamics.

ThestudyevaluatedtheeffectivenessoftheGametricssystemintwoexperiments.Thefirstexperiment involved 40 participants who played the games and had their behavioral biometricdatacollected.Thedatawasanalyzedtodeterminetheaccuracyofthesysteminidentifyingtheparticipants.Theresultsshowedthatthesystemachievedanaccuracyrateof93.75%.

The second experiment involved a simulated attack scenario in which an attacker attemptedtoimpersonatealegitimateuserbyplayingthegames.TheresultsshowedthattheGametricssystemwasabletodetecttheattackwithanaccuracyrateof95%.

The Gametrics system provides a promising approach to enhance the security of behavioralbiometricauthenticationsystems.Theuseofsimplecognitivegamesmakesthesystem non-intrusive and user-friendly while still providing strong security. The study demonstrates theeffectivenessofthesysteminidentifyinglegitimateusersanddetectingattacks.

Asghar et al. (2018) proposed a multimodal biometric authentication system that combinesgametrics with facial recognition. The system uses a set of cognitive games to collectbehavioral biometric data and a facial recognition system to collect physiological biometricdata.Thedatacollectedisthenfusedatthedecisionleveltoauthenticatetheuser.Thestudydemonstratedthatthesystemachieveshigheraccuracythanusingeithermodalityalone.

Weng et al. (2019) proposed a gametrics-based keystroke dynamics authentication system.The system collects behavioral biometric data through a set of games that require users totype specific phrases. The data is then analyzed to identify unique keystroke dynamicspatterns of the user. The study demonstrated that the gametrics-based keystroke dynamicssystemprovideshigheraccuracythantraditionalkeystrokedynamicssystems.

Hu et al. (2020) proposed a gametrics-based gait recognition system. The system collectsbehavioral biometric data through a set of games that require users to walk or performspecific movements. The data is then analyzed to identify unique gait patterns of the user.The study demonstrated that the gametrics-based gait recognition system provides higheraccuracythantraditionalgaitrecognitionsystems.

Wangetal.(2019)proposedagametrics-basedvoicerecognitionsystem.Thesystemcollectsbehavioralbiometricdatathroughasetofgamesthatrequireuserstospeakspecificphrases.Thedataisthenanalyzedtoidentifyuniquevoicepatternsoftheuser.Thestudydemonstrated that the gametrics-based voice recognition system provides higher accuracythantraditionalvoicerecognitionsystems.

Combining gametrics with other biometric modalities provides a promising approach toenhance the security of authentication systems. The use of multiple modalities provideshigher accuracy and resilience to attacks. Future research can explore the feasibility andeffectiveness of combining gametrics with other biometric modalities in various applicationscenarios.[38-41]

2. EXISTINGSYSTEM

FollowingarethepaperswhereUserauthenticationisperformedbasedonKeystrokedynamics and Game behaviour biometrics. But as per our knowledge and Literature SurveytherearenoworkspublishedwiththecombinationofKeystrokedynamics,MousedynamicsandGamebehaviourdynamics.

"Gamification with Keystroke Dynamics for User Identification" by Rafael Dueire Lins,CristianoAndrédaCosta,RodrigoEliaAssad,andLuizOlavoBoninodaSilvaSantos.In

this paper, the authors propose a gamification approach that combines keystroke dynamicsandgamebehaviorforuseridentification.Theproposedapproachinvolvesdesigningag amethat requires users to type specific phrases, and their keystroke dynamics are used to verifytheiridentity[16].

"Game-BasedAuthenticationUsingKeystrokeDynamics"byWeiXiong,JunjieZhang,andXiangyang Luo. This paper presents a game-based authentication system that combineskeystrokedynamicsandgamebehavior.Thesystemusesagameinterfacetocollectkeyst rokedataandanalyzeittoverifytheuser'sidentity[17].

"KeystrokeDynamicsandGameBehavior:TowardsaHybridUserAuthenticationScheme"byTa rekBejaoui,AhmedHadjKacem,andMohamedMosbah.Thispaperproposesahybriduser authentication scheme that combines keystroke dynamics and game behavior. Theproposedschemeinvolvesdesigningagamethatrequiresuserstotypespecificphrases,andthei rkeystrokedynamicsareusedtoverifytheiridentity[18].

"AGame-BasedAuthenticationSystemusingKeystrokeDynamics"byAliAwad,AmrAbdEl-Wahab, and Hoda Onsi. This paper presents a game-based authentication system thatcombines keystroke dynamics and game behavior. The system uses a game interface tocollectkeystrokedataandanalyzeittoverifytheuser'sidentity[19].

3. PROPOSEDSYSTEM

Theideaistoauthenticatetheuserwithhelpofacrosswordpuzzle.Puzzlecomprisesofanswers which can be of both typed and clicked. While the user plays a game i.e., solves across word puzzle, his game behavior, mouse behavior and key behavior will be extracted.TheCrosswordpuzzlewillactasasimplegametoderivetheuser'sanalyticalandcognitiv eskills.Whileusertypestheanswer,keydynamics willberecorded. Whileuserclicksonthehints,mousedynamics willberecorded.Thewholegameplayingbehaviorwillberecordedandwillbesavedasuser'sGame tricsbehavior.

Duringregistrationphase,theuserneedstosolverandomlygeneratedpuzzlesforatleast15 times, only 3 times per day, in order to perfectly extract the key stroke, mouse and gameplayingbehaviors.Thepuzzleswillappearinrandomway,asrandomnessincreasessecuritya gainst spoofing attacks increases. A template will be created for every user with all theextracted behaviors and will be saved to a database for later use. Separate templates will becreated for every Behavioral Biometric. During authentication phase, the user will solve thepuzzle. All the three templates will be matched against their respective templates and if amatch turns out to be successful, the user gets authenticated. Decision level fusion will betakenplacewheregametricsmatchdecisionandirismatchdecisionwillbeconjugatedandafinal decisionwillbetaken[20,21].

Followingisabriefelucidationoftheselectedtraitsfromtheuserbehavior.

S.No	Biometrictrait	FeatureName	Details
1.	Keystrokedynamics	Firstkeystroke	Timeatwhichkeystrokewasfirstoccured
2.		Dwelltime	LatencytimebetweenKPandKR
3.		Flighttime	LatencytimebetweenKRtonextKP

4.		Seektime	LatencytimebetweenKRandsuccessiveKP
5.		DigraphPresstime	LatencytimebetweenKPandsuccessiveKP
6.		Total keystroke duration	Totaldurationoftimewherekeyswereinput
7.		Keystrokespeed	Speedorrateatwhichkeysweretyped
8.	Mousedynamics	Totaldistance	Totaldistancethemousehaswandered
9.		Averagespeed	Averagespeedduringmousemovement
10		Averageacceleration	Average acceleration during mousemovement
11		Clicksilence	Silenecebetweensuccessiveclicks
12		Xaxisdifference	DifferencebetweenblockstartandclickinXaxis
13		Yaxisdifference	DifferencebetweenblockstartandclickinYaxis
14	Gamedynamics	Timeduration	Totaltimeelapsedtosolvethepuzzle
15		Firstactiontime	Firstmouseclicktimestampafterpuzzlestarts
16		Errors	Numberofmistakesattempted

4. METHODOLOGY

TheapplicationGUIand logicisbuiltinJavaprogramminglanguageandMySQLisused to store the questions repository and the user behaviour templates. The Key strokedynamics and Game behaviour dynamics are recorded with help of Thread, ActionListener,KeyListener,FocusListenerfacilitiesinJava.Therecordedvaluesaresavedintothedatabasefromthe UserInterfacewiththehelpofJDBC.

The application generates crossword puzzle from the questions saved in MySQLdatabase.Thedatabaseconsistsofhugerepositoryof1000+custommadequestionsfromthefieldsGeneral,Mathematics,ScienceandSocial.Thequestionsarepickedfromthesubjectschosenbytheuserwhile registration.

Algorithmtogenerateacrosswordpuzzle

STEP1:Chooseagridsize:Decideonthesizeofthegridyouwanttouseforthecrosswordpuzzle.

STEP2:Determinetheplacementofthelongestwords:
Choosethelongestwordsyouwanttouseinthepuzzleandplacetheminthegridsothattheyintersectwitheachother.

STEP3:Generateawordlist:Createalistofwordsthatyouwanttoincludeinthecrosswordpuzzle.Thewordsshouldberelevanttothethemeofthepuzzle,andofvaryinglengths.

STEP 4: Fill in the grid with words: Start with the longest words first and fill in theintersections with shorter words that fit the spaces. Continue filling in the grid with wordsuntilallthespacesarefilled.

STEP5:Checkforconflicts:Makesurethatallthewordsintersectingeachotherformvalidwords.Ifanyconflictsarise,rearrangethelettersuntiltheyformvalidwords.

STEP 6: Display clues: Display clues for each word in the crossword puzzle. The cluesshouldbesimpleandstraightforward,butchallengingenoughtokeepplayersengaged.

STEP7:Finalizethepuzzle:Makeanynecessaryadjustmentstothegridandclues,sothatallareclearandsolvable.

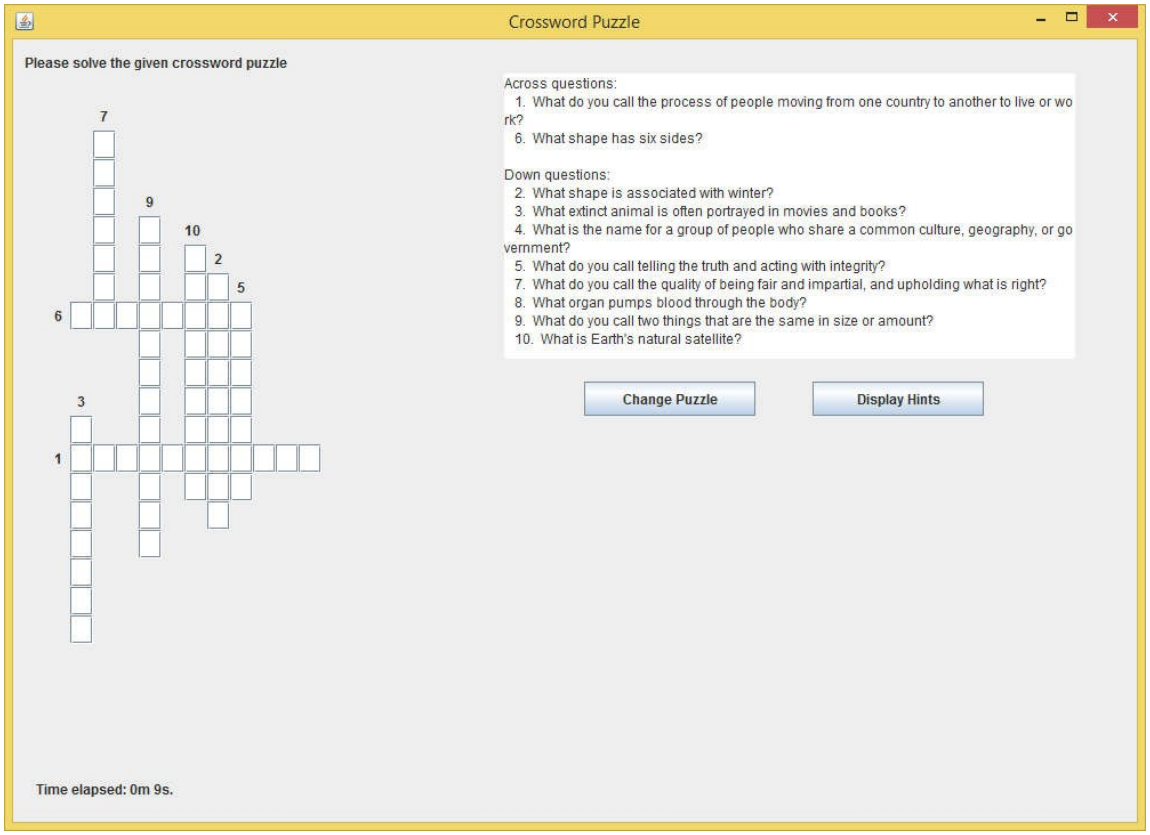

Fig.1.ExpectedCrosswordpuzzleUserInterface

AveragePuzzlegenerationtimewith10numberofquestionsis10milliseconds.

While the user tries to solve the puzzle, The game behaviour and the Keystrokebehaviour will be parallelly recorded and save to database. The user is said to solve thepuzzle for atleast 15 number of times and only 3 times per day. In this way, the generatedunique template will be free from any bias. The generated templates should be normalizedbefore generating a unique template because behavioural biometrics values get effected byfactors such as Physical factors, Environmental factors, Emotional factors, Habitual factors,Intentionalfactors.

5. EXPECTEDOUTPUT

Theproposedsystemshouldbeabletoperfectlyauthenticatevalidiuserswithregistered behaviour and reject unauthenticated users. False Acceptance Rate and FalseRejection rate of the application should be at minimum and the performance should be veryfastandaccurate.

6. CONCLUSION

With today's increasing demand on dependable and secure systems, stronger andmore secure authentication mechanisms are required. Designers of such systems strive toincorporate technologies that are usable, less intrusive, and more secure. Biometric systemsaregoodcandidatesforsuchpurpose.Theaccuracyofbiometricsreliesonthematurityofth emodelusedandhowaccurateitisincapturingdifferenthumancharacteristics.

REFERENCES

1. *Jain,A.K.,Ross,A.,&Nandakumar,K.(2016).Introductiontobiometrics.Springer.*
2. *Li,X.,&Jain,A.K.(2011).Handbookoffacerecognition.Springer.*
3. *Rathgeb, C., & Busch, C. (2018). On the vulnerability of fingerprint recognition systems to fakefingerprints.IEEETransactionsonInformationForensicsandSecurity,13(5),1111-1126.*
4. *Monwar, M. M., & Bhuiyan, M. Z. A. (2018). Multimodal biometric authentication using fingerprintand iris recognition. In 2018 International Conference on Electrical, Computer and CommunicationEngineering(ECCE) (pp.1-6).IEEE.*
5. *Akhtar, Z., & Khalid, S. (2019). Face recognition based biometric authentication system using deeplearning.In20193rdInternationalConferenceonIntelligentComputingandControlSystems(ICICCS)(pp.994-998).IEEE.*
6. *"AReviewofBiometricTechnologyalongwithTrendsandProspects"byTanviretal.,publishedintheInternati onalJournalofEngineeringandAdvancedTechnology(2018).*
7. *Rattani, A., Deravi, F., & Malaquias, I. (2016). A survey of biometrics: Concepts, applications andchallenges.JournalofCommunicationsandInformationNetworks,1(1), 1-18.*
8. *Carmona-Duarte, C., et al. (2021). Deep Learning Approach for Keystroke Dynamics-Based UserIdentification. AppliedSciences,11(3),1178.*
9. *Monrose, F., et al. (2000). Keystroke Dynamics as a Biometric for Authentication. Future GenerationComputerSystems,16(3),351-359.*
10. *Othman, Z. A., et al. (2016). A Hybrid Feature Selection Technique for Keystroke Dynamics-BasedUserAuthentication.InformationSciences,372,618-631.*
11. *Wang, Y., et al. (2020). Continuous Mobile User Authentication via Keystroke Dynamics. Sensors,20(19),5632.*
12. *Ullah, A., et al. (2018). Game behavior biometrics for user identification and authentication. IEEETransactionsonInformationForensicsandSecurity, 13(9),2257-2271.*
13. *Chang,K.,etal.(2018).Gameplaypatternsasanindicatorofcognitiveoverloadandstressinplayers.Entertain mentComputing,28,44-50.*
14. *Hajizadeh, S., et al. (2019). Using game behavior biometrics for personalized gaming experiences.Proceedingsof the2019IEEEConference onGames(CoG),1-8.*
15. *Cretu, V., et al. (2020). Monitoring cognitive decline in older adults using game behavior biometrics.JournalofAmbientIntelligenceandHumanizedComputing,11,513-527.*
16. *Lins, R. D., da Costa, C. A., Assad, R. E., & Santos, L. O. B. D. S. (2019). Gamification with KeystrokeDynamics for UserIdentification.In2019 IEEE InternationalConference on Systems,ManandCybernetics(SMC) (pp.1344-1349).IEEE.*
17. *Xiong, W., Zhang, J., & Luo, X. (2016). Game-Based Authentication Using Keystroke Dynamics. InProceedingsofthe2016ACMConferenceonMultimediaConference(pp.1459-1468).ACM.*
18. *Bejaoui,T.,Kacem,A.H.,&Mosbah,M.(2019).KeystrokeDynamicsandGameBehavior:TowardsaHybrid User Authentication Scheme. In International Conference on Security and Cryptography (pp.111-122).Springer.*
19. *Awad,A.,AbdEl-Wahab,A.,&Onsi,H.(2018).AGame-BasedAuthenticationSystem usingKeystrokeDynamics.In2018InternationalConferenceonInnovativeTrendsinComputerEngineering(ITCE) (pp.1-6).IEEE.*

20. *Manar Mohamed, NiteshSaxena.,Gametrics: towards attack-resilient behavioral authentication withsimplecognitivegames.,InProceedingsofthe32ndAnnualConferenceonComputerSecurityApplications,AssociationforComputingMachinery,NewYork,NY,USA,277–288.DOI:https://doi.org/10.1145/2991079.2991096(2016)*
21. *Sindhu. B, Kezia. Rani. B, "Augmenting Biometric Authentication with Artificial Intelligence," 2021,IEEE Xplore, 4th International Conference on Recent Trends in Computer Science and Technology(ICRTCST), 2022,pp.340-347, doi:10.1109/ICRTCST54752.2022.9781908.*
22. *Carmona-Duarte, C., et al. (2021). Deep Learning Approach for Keystroke Dynamics-Based UserIdentification. AppliedSciences,11(3),1178.*
23. *Monrose, F., et al. (2000). Keystroke Dynamics as a Biometric for Authentication. Future GenerationComputerSystems,16(3),351-359.*
24. *Othman, Z. A., et al. (2016). A Hybrid Feature Selection Technique for Keystroke Dynamics-BasedUserAuthentication.InformationSciences,372,618-631.*
25. *Wang, Y., et al. (2020). Continuous Mobile User Authentication via Keystroke Dynamics. Sensors,20(19),5632.*
26. *Sae-Bae,T.,etal.(2015).Anevaluationofmousedynamicsasabehavioralbiometricforauthentication.InternationalJournalofInformationSecurity,14(2), 97-107.*
27. *Ahmed, M., et al. (2018). Biometric authentication using keystroke and mouse dynamics: A novelapproach.InternationalJournalofAdvancedComputerScienceandApplications,9(2),58-64.*
28. *Jain, S., et al. (2017). Continuous authentication using mouse dynamics: A comprehensive study. IEEETransactionsonInformationForensicsand Security, 12(2),371-384.*
29. *Monaco, J., et al. (2019). A long-term evaluation of mouse dynamics as a biometric modality. IEEETransactionsonInformationForensicsandSecurity, 14(8),2004-2016.*
30. *Ullah, A., et al. (2018). Game behavior biometrics for user identification and authentication. IEEETransactionsonInformationForensicsandSecurity, 13(9),2257-2271.*
31. *Chang,K.,etal.(2018). Gameplaypatternsasanindicatorofcognitiveoverloadandstressinplayers.EntertainmentComputing,28,44-50.*
32. *Hajizadeh, S., et al. (2019). Using game behavior biometrics for personalized gaming experiences.Proceedingsof the2019IEEEConference on Games(CoG),1-8.*
33. *Cretu, V., et al. (2020). Monitoring cognitive decline in older adults using game behavior biometrics.JournalofAmbientIntelligenceandHumanizedComputing,11,513-527.*
34. *Monrose, F., &Rubin, A. (1999). Keystroke dynamics as a biometric for authentication. FutureGenerationComputer Systems,16(3),351-359.*
35. *Shirazi, H., Shirazi, B., & Shirazi, A. (2011). Continuous user authentication using keystroke andmousedynamics.Journalof Networkand ComputerApplications,34(5),1460-1469.*
36. *Sae-Bae, N., & Suksomboon, A. (2014). Keystroke and mouse dynamics for user authentication usingmachine learningalgorithms.Computers&Security,42, 60-69.*
37. *Alzahrani,A.,&Almuairfi,A.(2020).Continuousauthenticationofmobiledeviceusersusingkeystroke and mouse dynamics. Journal of Ambient Intelligence and Humanized Computing, 11(11),5221-5235.*
38. *Asghar, H. J., Al-Assam, H., & Ahmed, S. F. (2018). Multimodal biometric authentication usinggametricsandfacial recognition.IEEEAccess,6, 14764-14772.*
39. *Weng, J., Li, J., Huang, C., & Sun, X. (2019). A gametrics-based keystroke dynamics authenticationsystem.IEEEAccess,7,36551-36561.*
40. *Hu,Y.,Liu,Y.,&Yu,Z.(2020).Gaitrecognitionbasedongametrics.IEEEAccess,8,184023-184033.*
41. *Wang, Q., Liu, H., Xu, L., Zhao, Y., & Wang, C. (2019). Gametrics based voice recognition system. In2019 IEEE 6th International Conference on Cloud Computing and Intelligence Systems (CCIS) (pp.47-51).IEEE.*