IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON MOBILE MULTIMEDIA: METHODOLOGY AND APPLICATIONS

Received December 16, 2019, accepted December 28, 2019, date of publication January 1, 2020, date of current version January 8, 2020.

Digital Object Identifier 10.1109/ACCESS.2019.2963543

Doodle-Based Authentication Technique Using Augmented Reality

WAQAS WAZIR[1], HASAN ALI KHATTAK[1], (Senior Member, IEEE), AHMAD ALMOGREN[2], (Senior Member, IEEE), MUDASSAR ALI KHAN[3], AND IKRAM UD DIN[3], (Senior Member, IEEE)

[1]Department of Computer Science, COMSATS University Islamabad, Islamabad 44550, Pakistan
[2]Chair of Cyber Security, Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia
[3]Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan

Corresponding author: Ahmad Almogren (ahalmogren@ksu.edu.sa)

This work was supported by the Deanship of Scientific Research, King Saud University, through Vice Deanship of Scientific Research Chairs.

ABSTRACT The emergence of augmented reality (AR) and virtual reality (VR) has revolutionized the trends in computing devices and modern technologies drastically. With this revolution, there is a need to extend existing architectures of security to serve as the key protective feature in all computing devices. In this experimental study, the aim is to develop a novel authentication technique with a fusion of graphical doodle password approach and AR environments. The mash-up of both doodle passwords and AR in a 3D space gives a promising direction to set off to a modern, more usable, and satisfying authentication techniques. The proposed approach works on real-time size and coordinate matching of doodles in an AR environment for the authentication of users. The creation of doodle passwords in an AR space is carried on by touch-gesture-recognition on a smartphone. The usability and usefulness of the proposed technique is evaluated by conducting an extensive survey, based on tasks and user experience assessments. The randomized-post-test-only study model is used to conduct experimentation that is also followed by the analysis of security parameters with the help of confusion matrix. The obtained results predict the use of AR during the authentication process more satisfying for users, where the proposed technique is useful, usable, and secure in comparison to the existing authentication approaches. This paper also highlights the importance of research needed for the utilization of modern techniques during the creation of security frameworks.

INDEX TERMS Augmented reality, gesture recognition, password, doodle-based authentication, usable security.

I. INTRODUCTION

Authentication serves as a prime shield for computing devices and systems. The ultimate goal for authentication is to identify between authorized and unauthorized access (either by entity or process). Only strong authentication techniques and efficient access control models can help in better tracking and denial of unauthorized access for any smart devices or systems. Having said that users still risk their security mostly just because of inconvenient or less usable authentication methods [1], [41].

To overcome the inconvenience, it is the need of the hour to focus attention towards techniques that are more reliable, difficult to compromise, and most importantly easy to use so that users can focus more on activities behind the authentication and not on the apparent authentication interface [4]. One of the most demanding techniques for authentication is the gesture-based authentication. Above all, an authentication technique is useful only if it is fulfilling its primary purpose of security and is usable. According to [5], the cracking of passwords based on doodles is more difficult and are thus reliable and secure. The creation of various possibilities of the same doodle may exist but more in numbers in comparison to the text-based traditional password schemes. Text or PIN based passwords or pass-phrases always come from a language, such as English, and have the known number of digits, e.g., 4 Digit PIN etc., making it prone to dictionary attacks or brute force attacks.

The associate editor coordinating the review of this manuscript and approving it for publication was Danda Rawat.

Amongst the list of modern technologies, augmented reality (AR) has a great deal of technological advancement that has picked up its pace in the recent years and it is still going to be one of the leading technologies in the near future. AR is comprised of the following main attributes [2]: 1) A representation of both real and virtual world is provided, 2) The representation is interactive in nature, 3) The environment is registered as a three dimensional space. AR does not eliminate the user from reality. Instead, it augments the virtual content onto the real world. Thus providing the precise real-time alignment of real and virtual environment at the same instance. The features of AR dramatically increases its utility as it does not affect the work-flow; without taking away the user from reality [3]. Augmentation of reality opens up door to numerous application area like gaming, designing, design mapping, planning, interactive learning, etc.

The motive for the proposed study is to develop a touch-gesture-based authentication technique based on doodles by using AR, keeping in view the convenience and security of the user. This study also highlights that the use of AR for security can lead us to a new direction for providing cyber-security that will not only be secure and useful but will also be an amusing and satisfying for users. The rationale behind this research is to answer the following research questions:

1) Can AR be used to develop a new authentication technique?

2) Does doodle drawn in an augmented environment be secure and usable for authentication?

3) Can doodle-based authentication using AR provide a better and more satisfying user experience in comparison to existing approaches such as PIN codes, Text base passwords, and Swipe-based-Pattern Locks? To explore these questions, a treatment experimental setup using GoogleCreativeLab known as AR Drawing is created. New features of doodle creation authenticated by matching of doodles are created in the proposed technique. A novel algorithm is also proposed for authentication in a real-time AR environment by doodle matching to keep a similarity threshold index. The proposed technique is intended to provide better user experience along with security, usability, and usefulness. For the experimentation of selected measures triptych model of interactivity [28] and confusion matrix [29] are used and the research model of Randomized-Posttest-Only Research Design [30] is followed to conduct an appropriate and useful evaluation. The experimentation is carefully conducted by a user-centric evaluation survey through a questionnaire assisted by tasks to evaluate selected measures. In order to present the study efficiently, it is structured in three major parts. The first part describes the literature review providing an overview of existing authentication techniques with their prominent aspects. The second part explains the proposed technique and methodology along with the details of evaluation and analysis of results. The last part provides conclusion and outlook to some of the future work that we think should be given importance.

II. LITERATURE REVIEW

With the exponential growth of information, access to information ratio has increased tremendously. This phenomenon raises questions about the authentication and authorization of users before they access any private information. In 1960s, IBM formalized different authentication factors for confirming the identity of a person in a digital environment to provide it with the access to digital information or system [6], [7].

- **Knowledge Factor** This factor is about acknowledging Something You Know (Recall). Examples for this factor include passwords and Personal Identification Numbers (PIN). Authentication factors of this kind are kept on the basis of Secret that is shared between both the entities, the one who is accessing the digital information, e.g., user and the one granting access to any information, i.e., system or application. These secrets at times can be Passwords, Graphical passwords, PIN codes, Patterns, etc.
- **Ownership Factor** This factor relates to Something You Possess/Have. Ownership factor use tokens/keys/certificates for authentication that user possess. These possessions may be ID card, passport or smart card with embedded microprocessor chip which users may carry to present for authentication.
- **Inherence Factor** This factor refers to Something You Are/You Do. Gestures (gate/walk modeling), DNA and most importantly all kind of biometric information are example of inherence factor.

Biometrics measure unique physical and behavioral characteristics of the user. Physical characteristics include fingerprint, iris and facial scans, and are referred to as static biometrics. While the behavioral characteristics include handwritten signatures and gestures that a user repeatedly performs in order to get authenticated or carry out certain actions.

In this study, we focus on touch-gesture-recognition of the inherence factor. Out of these varieties of authentication schemes, we discuss a hybrid approach blending in graphical authentication and gesture recognition schemes in an AR environment.

A. GRAPHICAL AUTHENTICATION SCHEME

Graphical authentication schemes use pictures and drawings as passwords [8], and are further sub-divided into recognition based, cued recall based, and pure-recall based techniques. The following subsections define each one briefly for their respective properties.

1) RECOGNITION BASED TECHNIQUE

In this scheme, users are presented with a set of images and in order to get authenticated, they have to select the same images they have selected at the time of registration [8]. Recognition based technique further consists of various schemes, which are discussed below:

A scheme is proposed in [9] using images for authentication (Visual Memory) that makes users choose certain pictures from a dataset of random images and then to authenticate them, it must re-select the previously selected images in the similar order.

Another scheme called Passfaces authenticates users when they re-select four images of human faces selected at the time of registration from the grid of nine human faces [10].

An authentication approach is proposed in [11], which is about scattering *N* numbers of distinguishable unique objects (may be 100 or 1000) on the screen. Users then select random three objects at the registration phase. Whereas for authentication, they have to identify those previously selected objects that will be making an invisible triangle and they have to click inside it. It is just like clicking inside the convex hull of pass-objects.

2) CUED RECALL BASED TECHNIQUE

In the techniques based on cued recall, users have to reproduce (with the help of given hints and clues) what they have selected or created earlier at the time of registration [8], [12]. Users are provided with the some hints or clues at the time of authentication. Several different schemes work on the recall-based technique, such as Blonder, Passpoint, Passlogix v-Go, and A Novel 3D Graphical Password Schema.

Blonder method [13] authenticates a user by presenting a pre-determined image having pre-arranged points, regions or areas, and the user must locate the points, regions or areas in the pre-determined order.

In the Passpoint scheme [14], a user has to select click points on a given image in some sequence and for authentication has to repeat the same sequence by clicking same points in same order.

Passlogix v-Go [15] is another authentication cued recall-based approach created by Passlogix Inc, which is a private security company based in New York City, USA. This scheme uses a technique called ''Repeating a sequence of actions'' in which users select a background image and then click/drag a number of items within that pictures to create a password. Whereas for authentication, the same chronological order of clicking/dragging of items is performed at the registration phase.

A novel 3D graphical password scheme, proposed and evaluated in [16], gives privileges to users of selecting any of the authentication technique as their 3D password. The 3D password authentication needs both recognition and recall-based techniques for authentication. In order to set passwords, users can freely navigate and roam around in a virtual interactive environment and thus can interact with various objects in the provided 3D space in a specific sequence, which is captured by various input devices. Every object in a 3D environment possesses its own (x,y,z) coordinates. For authentication, a user has to re-interact with the 3D digital interactive environment in the similar fashion as did before at the time of registration [16].

3) PURE RECALL BASED TECHNIQUE

Pure recall-based technique is the same as the cued recall-based technique. The only difference between the two is such that the cued recall-based provides some hint to users for authentication while the pure recall based-does not provide it.

As proposed in [17], the authentication of hand drawn doodles created using mouse is performed where doodle similarity with already registered doodle as well as the speed of creating the doodle is kept as major measures. Initially the doodle being authenticated is scaled and stretched to a grid. Then the comparison is created against the distribution gird previously stored at registration phase. Further instantaneous speed is compared at various point of doodle drawing process. For being successfully authenticated, a user must redraw the same Passdoodle provided at the time of registration.

Draw A Secret (DAS) [18] method prompts end users to first draw passwords on the two dimensional grid. The grid is mainly of G×G size and every cell member inside the provided grid is accessible with discrete coordinates (x,y). To clear the phase of authentication, users must match the order of selecting the discrete coordinates as already saved in the phase of user registration.

In Grid Selection, proposed in [15], a user initially selects a drawing grid from a large, fine grained selection grid to zoom in and draw a password. This technique works the same as the DAS technique but it also increases the DAS password space.

In [20], the algorithm Syukri is proposed that works on the creation and authentication of users with signatures drawn by pointing devices, for example, mouse. The system has two main phases, namely user registration and verification. In the phase of user registration, a signature is drawn into the system by the user. The area of signature is then extracted by the system and the signature is then normalized, i.e., either increase or scale-down and also rotate if needed. All the signature related information is saved inside a database. Later, during the phase of user verification, similarly as the registration phase, the user is prompted to re-create the signature. The signature area is minimized and normalization is performed for the selected region where unnecessary information associated with the signature is removed. The authentication system then conducts a verification process using geometric formula such as geometric average, means, etc., and also a dynamic update is performed at the end of database.

B. GESTURE RECOGNITION SCHEMES

Universally, there is no agreed upon terminology for gesture types [4]. Different names for the same gesture types are used at various points of the literature. An overall view of gesture recognition, through one prospective, can be structured into mainly two categories, i.e., touchscreen gestures and motion gestures.

Touchscreen gestures are those which are captured through the touchscreen. They can be single stroke gestures, multi stroke gestures, and multi touch gestures. In single stroke

gesture based systems, users perform continuous input on the screen mostly using only one finger, while in multi stroke gestures, multiple stroke attempts are allowed before the completion and are discontinuous. In contrast with the single touch gestures, multi touch gestures use more than one fingers to interact with the touch screen [4].

The recognition of motion gestures have two major types: sensor-based and camera-based motion recognition. Accelerometer, gyro sensors of the smartphone are at times used to capture user motions [4].

1) SWIPE BASED PATTERN AUTHENTICATION TECHNIQUE

Pattern authentication technique in android smartphones is also a knowledge-based graphical scheme that works by recognizing touch gestures. This technique presents a user with a 3×3 grid where the user draws pattern by connecting points in the grid. This scheme is adaptable in a way that it let the user create simple but also fairly complex gestures [23], [24].

2) GRAPHICAL RANDOMIZED AUTHENTICATION TECHNIQUE (GRAT)

A similar swipe-based authentication technique [35] is proposed where a user touches the screen for authentication. In contrast to existing approaches, rather than providing users with a simple 3×3 grid, image icons are given inside the grid. Instead of remembering the grid pattern, the user remembers the image icons and the order of their selection. During every authentication attempt, the user is provided with a randomly generated image icon grid that prevents the shoulder attack up to some extent. Thus, the user has to redraw a different design of pattern each time recalling the image icons and their order of selection.

3) SENSOR-BASED USER AUTHENTICATION

In this subcategory of gesture based authentication schemes, a specific sensor in mobile phones and smart devices are used during the authentication mechanism [22]. Gestures captured by such sensors vary for each user collectively that create different readings for users because of every user unique way of holding devices, unique structure of hands, size and flexibility variance between hands of different users. Such approaches motivate researchers to give importance to two major factors, i.e., to strengthen the sensors in smart devices to accurately recognize user hand gestures, and to consider biokinetics of hand during the process of gesture recognition.

4) AUTHENTICATION THROUGH HAND-GESTURE RECOGNITION

This technique authenticates users by measuring a 3D gesture performed by one of the user hands while holding a mobile device integrating accelerometer. The acceleration of the gesture movement in 3 axis in time is measured by accelerometer. According to this scheme, every person has a unique 3D associated hand gesture (like in the thin-air), created by itself, thus, the user is authenticated when the gesture is identified [21].

C. AUTHENTICATION SCHEMES USING AUGMENTED REALITY

All the existing authentication schemes are designed and tested in mainly two dimensional environments [23]. In case of 3D environment based authentication approaches, only a couple of virtual reality (VR) based approaches exist. One of the most closely related works is presented in [36], which proposed a hardware based door lock system using a four digit PIN code for a specific door. Unfortunately, the lock is missing the aspect of augmentation in reality. The proposed system searches for doors through the database and upon a correct user authentication through wireless communication, the door is unlocked. Conclusively, to the best of our knowledge, there is no user authentication approach that includes the augmentation of reality in real-time.

D. EXPLOITING INTERNET OF THINGS USING AUGMENTED REALITY

Due to the advancements in the past two decades, many connected devices that are smart in nature are being rapidly introduced to the market for end users. Most of them have the property of being communicated ranging from health, lifestyle, entertainment, etc. [38]. One of the key aspects behind this trend was the miniaturization of hardware and also rapidly evolving connectivity. Billions of users and devices are connected to the Internet, thus, forcing the phenomenon of Internet of Things (IoT). The things in IoT or devices that share the property of being computationally weak, have less storage space, and lack interfaces as compared to personal computers or smartphones [38]. As proposed in [39], a framework AR-IoT, there is a need to facilitate IoT with AR for creating IoT more interactive at various levels. Though the AR-IoT mainly focuses on gathering information from different objects inside an IoT structure, different objects may be controlled through the AR. For users to interact, control, and manage devices, they must be authenticated in prior to authorization [40].

III. PROBLEM DEFINITION

With the increase of smart devices, there is a need to continuously improve the authentication process for security and ease of use or usability in general. The existing gesture-based and graphical authentication schemes are prone to attacks and most importantly, with the increase in security of authentication approaches, the usability is lost [37]. One major aspect that requires more exploration is the use of modern technologies, such as augmented technologies, during the authentication process. The user authentication should be exploited using AR that will help not just user's satisfaction but would also assist in the IoT-based system where many things (devices) may lack proper interfaces due to their low computational strengths [38]. We hypothesize the use of AR-based authentication approach to be satisfying, usable, and necessary for authentication purposes.

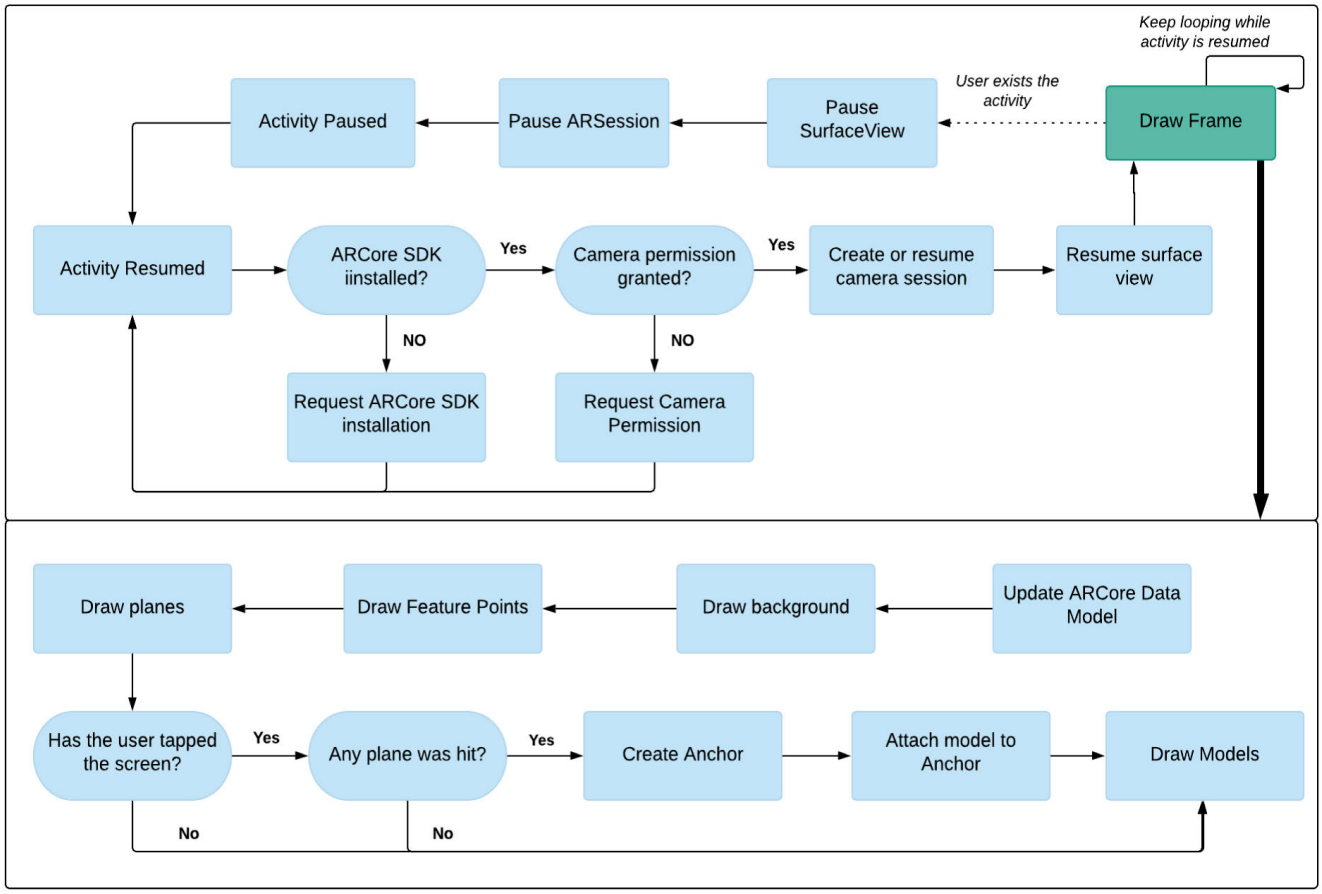


FIGURE 1. ARCore functionality flow.

IV. METHODOLOGY

The very essence of the proposed authentication technique is to amalgamate AR with doodle-passwords. For this purpose, we choose the AR implementation of Googlecreativelab called AR Drawing [36] and build the technique based upon it. The ARCore uses real-time camera feed from a smartphone to interact with the surroundings. First the real world coordinates are calculated on occurrence of touch event on the screen. Further image-processing, graphics libraries are used to create doodles on top of the measure real world coordinates.

On top of ARCore we generated doodles based on continuous single touch gesture recognition, further matching of doodles and authentication is performed via AR drawing. Inclusion of both the techniques give a full fledged doodle-based augmented reality experience for password authentication. "AR Drawing" set up the touch detectors, add strokes to the scene & 3D points to the strokes by continuously saving them.

A. PROPOSED ARCHITECTURE

The proposed architecture for the authentication scheme consists of logical, presentation, and data tier.

1) CREATING DOODLE STROKES IN SPACE

To create doodle strokes, the user touches the smartphone screen and moves it in the space in order to draw doodle shape, which will be set as a password. The user will draw five doodles in total, i.e., four for the registration and the fifth one for authentication. Fig. 2 shows the creation of three dimensional doodle strokes in space.

2) SAVING DOODLES FROM THE AR ENVIRONMENT

In order to register doodle shapes drawn in space, a user is given five turns to create the same very doodle five times. After the user completes, process of creating a doodle on the screen, the proposed system grabs the world coordinates(x,y,z) of the entire drawn doodle using vector math libraries which are normally using for visual programming. The (x,y,z) coordinates of these Registered Doodles are stored in a dynamic array lists (Vector 3f), which later are used during the similarity check in the authentication process.

3) RETRIEVING & AUTHENTICATING DOODLES

In order to authenticate a user, the designed authentication algorithm asks users to recreate the same doodle again, which was provided in the phase of user registration. This Drawn

FIGURE 2. Creating doodle strokes.

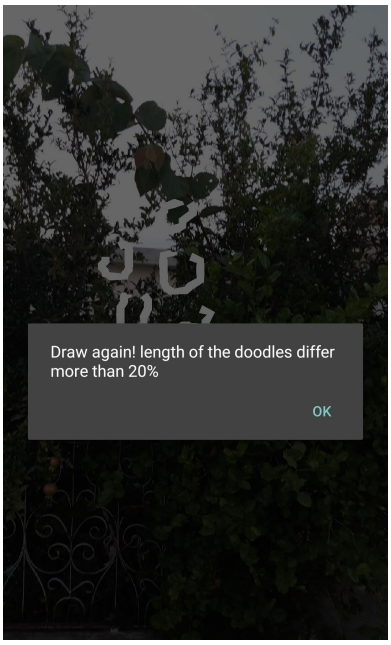


FIGURE 3. Difference in doodle length.

Doodle is then matched one-by-one with all five user Registered Doodles. The similarity is extracted by creating a difference among all coordinates.

In order to achieve the highest similarity, the Drawn Doodle should match Registered Doodles both in size and placement or content, i.e., coordinates(x,y,z). Five separate matching results are thus generated between the drawn and registered doodles. In order to handle incomplete attempts of re-creation of the doodles, 20% relaxation is kept. This means that if two doodles match up to 80% for their size, only then will be further checked for coordinates matching with all the five Registered Doodles. If this condition is not fulfilled, a user is alerted with the message "Draw again! Length of doodles differ more than 20%", as shown in Fig. 3.

In the next step of authentication, the difference between x, y, and z coordinates for all points of both the doodles, i.e., Drawn Doodle and Registered Doodles, is calculated and saved. To further conclude the matching results, the differences of all coordinates are added up to calculate the Sum of Differences. As recreating a doodle can be a complex task, a floating value of 0.001f is kept as the threshold, the maximum value for the Sum of Difference of doodles for a successful authentication. If the difference of x,y,z coordinates of both doodles is less than the threshold, a user is authenticated. This procedure would be carried between the Drawn Doodle and all the five registered doodles. The process may terminate with a prompt message if any successful match is encountered or in worst case if no successful authentication is performed, as shown in Fig. 4.

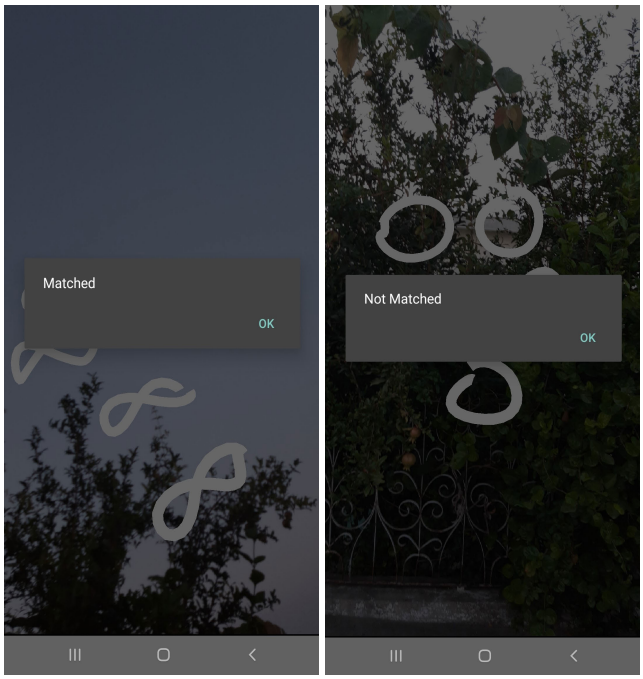


FIGURE 4. Matching doodle Strokes.

V. EXPERIMENTAL SETUP

The experimental setup for the proposed framework includes the formulation of a research design, evaluation axis, and sampling strategy adopted for evaluation. It also explains a survey with the help of selected research variables.

A. EVALUATION PARADIGM

The evaluation of any technique for validating its prime objectives is always a difficult task. Similarly, the selection of relevant evaluation standards is also a hard nut to crack. In 2004, an evaluation model used for interaction was proposed for digital libraries in specific [27], which introduced three main actors involved in the evaluation process, i.e., user, content, and system. Later on in 2007, the interaction Triptych model was proposed describing three evaluation axes defined by three entities (user, content, and system). That evaluation axes were usability, usefulness, and performance [28].

Another method to evaluate a certain measure for any system is confusion matrix, as discussed in [29]. Using confusion matrix, which acts like a classifying strategy, we keep the already known true values as a key set to analyze the correctness of the system.

We use the Tryptych model of interactivity [27] to analyze the measure of interaction authentication technique, i.e., usability and usefulness, keeping in view the objectives of the study. This model is selected for evaluation as it clearly defines the evaluation axis with respect to user, content, and system in addition to describe the criteria and sub-criteria for evaluating them. Moreover, the security aspect of the proposed technique is also evaluated using confusion matrix. The rational behind selecting this matrix is such that it clearly and precisely evaluates the given set of classified true and false inputs for measuring how much a system is secure.

B. RESEARCH DESIGN

In all kinds of research studies, establishing an effective research design holds significant importance in comparison to other parts of the study. This phase traditionally includes specification and design of the research structure that eventually leads to efficiency and productivity. We adopt the described research model of [30], which specifies experimental setup, mathematical analysis, and evaluation on the basis of gathered results.

We conduct an experimental research by performing a random sample selection and group testing. In this study, we have considered Randomized-Posttest-Only Research design, which has a combination of two groups namely control and treatment.

On the treatment group in this study, the proposed authentication is used, while the control group chooses to use any available existing authentication approach. In the end, both groups are scrutinized for a set of dependent variables. We have considered a case where 40 subjects are involved [30]. That is why, in the proposed study, we have randomly selected 20 participants for the control group and 20 participants for the treatment group out of the accessible population.

C. SAMPLING

For this study, the targeted people are the users who use smartphones and have acquired services of any kind of authentication application either builtin or third party. The undergraduate, graduate, and postgraduate students of the University of Haripur are the accessible population. Further to extract a suitable sample out of the accessible population, a two-stage sampling strategy was adopted. In the first phase, on the basis of convenience, three departments of the university were shortlisted, i.e., Department of Information Technology, Department of Management Sciences, and Department of Psychology. In the second phase, out of the student list provided by each department, 40 participants were randomly selected (upon availability) to participate in the study.

D. SURVEY

In this research study, we experimented a user-centeric evaluation based on Randomized-Posttest-Only Research design. For this purpose, we asked participants of both the groups a same set of questions and similar tasks. The description of each task is as:

- **Task 1:** Create a password including a simple geometrical line.
- **Task 2:** Using the authentication system, set a password that includes any geometrical shape.
- **Task 3:** Generate and authenticate a password that has a circle in it.
- **Task 4:** Validate a password that includes a star or diamond shape.
- **Task 5:** Include an infinity symbol while creating a password.

E. EXPERIMENTATION

The proposed study is user-centric examining the usefulness, usability, and security of the proposed authentication technique. In addition, the study includes treatment and control groups. The treatment group is treated with the proposed authentication technique with a little training about its working. A survey is conducted to extract information and feedback from users. A sample of 40 individuals was randomly selected for the experiment. The criteria of selection for both groups is same, i.e., a users must use smartphones and authentication apps, and have somehow knowledge about them. Both control and treatment groups comprise 20 individuals. These participants are analyzed by conducting a survey and a questionnaire is circulated among them to ask a few questions. The experimentation of both groups is concluded as:

1) CONTROL GROUP

Control group comprises 20 students randomly selected from three departments who were shortlisted upon convenience from the University of Haripur. Participants had to perform the above-mentioned tasks and then accordingly fill in the given questionnaire. The questionnaire was related to the usability and usefulness of the proposed technique and tasks were related to the creation and authentication of the password. All participants performed the tasks on their personal

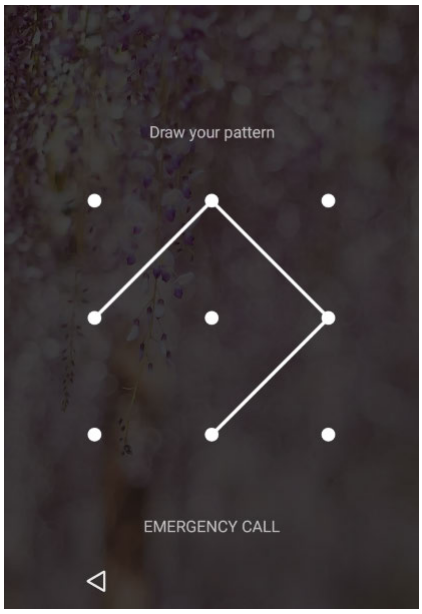


FIGURE 5. Pattern lock built-in authentication technique.

smartphones using Pattern Lock built-in app of their smartphones.

2) TREATMENT GROUP

The treatment group also had the same amount of 20 test subjects and the participants were randomly selected from three different departments of the University of Haripur. The participants performed the tasks by using a working prototype of the proposed technique of authentication based on AR. They were given a tutorial about the creation of password along with an overview of the interface. After this overview and tutorial, the participants were asked to perform tasks and filled-in the questionnaire.

The experimentation was subdivided into two major phases, i.e., performing the tasks and filling the questionnaire. The user evaluation primarily is based on the questionnaire, which has three parts. The first section was about profiling of participants; the second section focused on the usability of the proposed technique; and the focus of section three was the usefulness measure.

VI. EVALUATION AND RESULT ANALYSIS

The evaluation and analysis is the most crucial phase in the experimental research in which quality, goals, and objectives are studied to compare the results and outcomes. The evaluation is a systematic approach that analyzes any framework or architecture for its benefits and drawbacks, and a complete set of results should be followed to better demonstrate it [31]. A critical, unbiased, and fine-grained evaluation leads to proper results and significant outcomes.

Subsequent to describing the rationale behind selecting the triptych model [27] and confusion matrix [29], now we will explain the evaluation of the proposed technique and discuss the findings of evaluation in the form of quantitative results.

TABLE 1. Division of questions and tasks upon the evaluation axis.

Evaluation axis	Measures	Related Questions
4×USABILITY	Ease of Use	Q#6, Q#7, Q#8, Q#9
	Interactivity	Q#10, Q#11, Q#12
	Satisfaction	Q#13, Q#14, Q#15
	Effectiveness	Q#16, Q#17, Q#18, Q#19, Q#20
2×USEFULNESS	Utility	Q#21, Q#22, Q#23, Q#24, Q#25
	Relevance	Q#26, Q#27, Q#28, Q#29

A. ANALYSIS PROCESS

The term analysis refers to dividing a whole into parts aimed at understanding the parts' nature, functionality, and interrelationships [19]. The user-centric evaluation of study is performed on randomly selected participants on the basis of Randomized-Posttest-Only Research design. Both control and treatment groups are analyzed against research variables, as described in Table 1.

B. POSTTEST EVALUATION OF CONTROL & TREATMENT GROUPS

The participants of both groups were examined for different measures described in the following subsections in detail.

1) USABILITY

In this study, we choose the instrument of questionnaire to analyze the usability, and also backed by tasks to highlight the significance of the use of AR for better usability. Total 15 questions, as described in Table 1, and five tasks were discussed before the questionnaire was given to the participants of both control and treatment groups. The usability can be narrowed down into measures and further into submeasures as effectiveness, learnability, task completion time, satisfaction, etc. [28]. In the proposed study, the focus is only on the ease of use, interactivity, satisfaction, and effectiveness as usability measures.

a: EASE OF USE

Four questions related to ease of use were asked from participants of both test groups. Out of the total participants, 76% of the control group and 74% of the treatment group agreed that they needed to learn very less before using the system. Similarly, 78% of the control group and 82% participants of the treatment group stated that the functions in the app were well-integrated. Furthermore, 84% of the control group and 81% of the treatment group members shared the consent that understanding the interface of the system was easy for them. Likewise, 78% participants of both control and treatment groups stated that performing tasks while using the app was easy for them.

b: INTERACTIVITY

The participants of control and treatment groups were inquired about interactivity by asking three questions. Where 80% participants of the control group while 79% of the

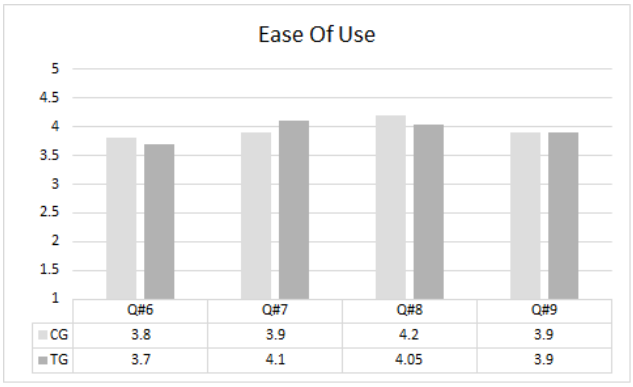


FIGURE 6. The ease of use comparison for control and treatment groups.

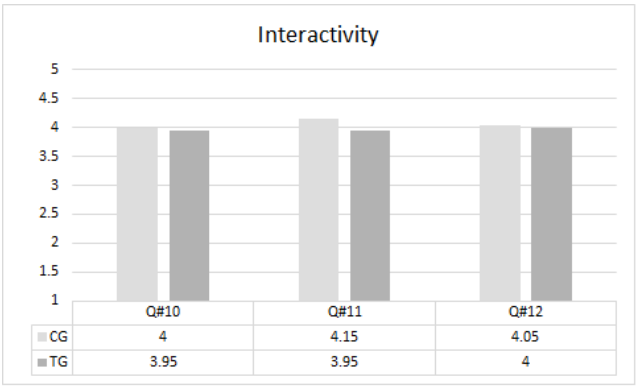


FIGURE 7. Interactivity comparison for control and treatment groups.

FIGURE 8. Satisfaction comparison of control and treatment groups.

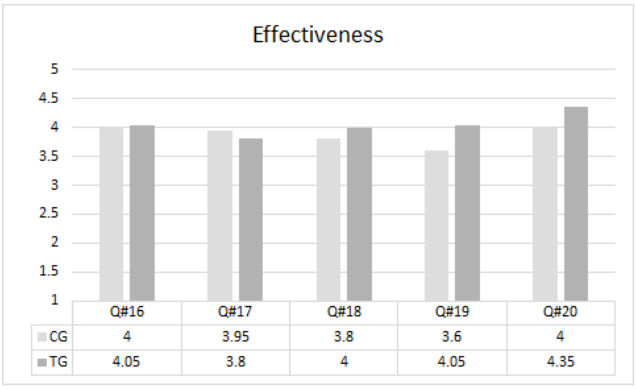


FIGURE 9. Effectiveness comparison of control and treatment groups.

treatment group agreed upon the clear response of the technique while performing tasks. In addition, 83% participants of the control while 79% of the treatment group stated that their every action was well-acknowledged while interacting with the app. Moreover, 81% participants of the control while 80% of the treatment group stated that that the app was well-structured and its key features were accessible.

c: SATISFACTION

The participants of both groups were inquired about their satisfaction while using the authentication technique by a set of three questions. The response of 81% of the control group and 84% of the treatment group was that they were satisfied with the experience of interacting with the app. Furthermore, 86% participants of the control group and 75% of the treatment group stated that the authentication process was simple and satisfying. According to 79% participants of the control and 75% participants of the treatment group, the process of password creation was not stressful at all.

d: EFFECTIVENESS

The effectiveness measure of usability was studied by asking total of five questions from participants. Amongst, 80% participants of the control group and 81% of the treatment group agreed that the app was performing all the functions effectively, i.e., producing the desired output. Out of the total, 79% participants of the control and 76% of the treatment group did not face any issue with the password creation and authentication process. Similarly, 76% of the control group and 80% of the treatment group agreed that the output was accurate and timely. Likewise, 72% participants of the control group and 80% of the treatment group did not come across any failure (any bug, error or no-output) while using it. Further, 80% of the control group' participants while 87% of the treatment group acknowledged that the app performs well while creating and authenticating the password.

2) USEFULNESS

The usefulness measure was studied by asking a set of nine questions from the participants. It constitutes two sub-measures utility and relevance for better evaluation.

a: UTILITY

The participants were asked about the utility of the system with five questions, where 82% of the control group and 84% of the treatment group agreed that the addition of new features can increase the utility of the technique. To add more, 75% of the control group and 87% of the treatment group suggested that there was a need for the AR/VR based authentication technique. In addition, 90% participants of the control group and 88% of the treatment group stated that a new technique must be more creative and attractive. Similarly, 87% participants of the control group and 79% of

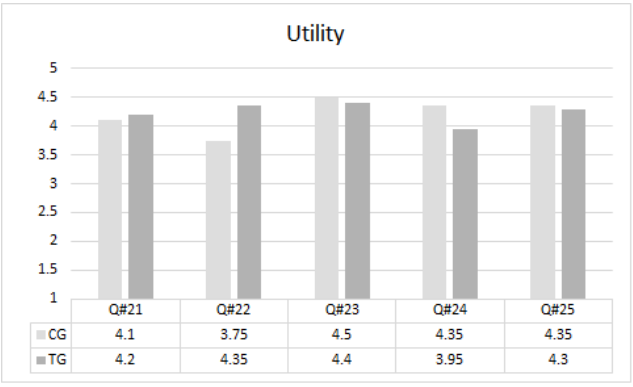


FIGURE 10. Utility comparison of control and treatment groups.

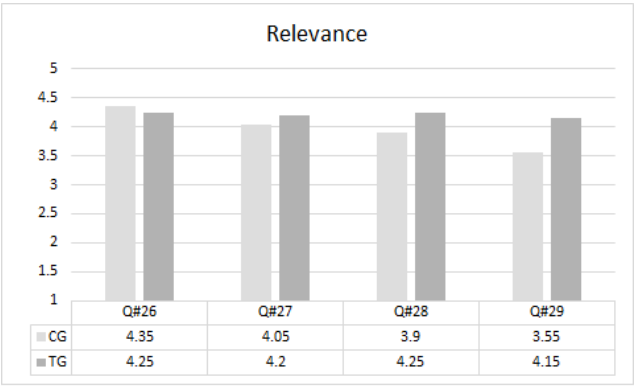


FIGURE 11. Relevance comparison of control and treatment groups.

the treatment group agreed that gesture-based authentication can provide more leisure to the authentication process. Correspondingly, 87% participants of the control group and 86% of the treatment group stated that gesture-based authentication in a 3D space using AR/VR environment would be new and innovative advancement in the existing authentication techniques.

b: RELEVANCE

The relevance sub-measure of the usefulness was examined by asking a set of four questions from the participants, where 87% of the control and 85% of the treatment group stated that the AR/VR based authentication provides better user experience and security while making it more useful than the existing techniques. Additionally, 81% participants of the control while 84% of the treatment group stated that the AR/VR based authentication technique will contribute well in the existing authentication techniques. Similarly, 78% participants of the control and 85% of the treatment group felt that the app that they are using is a modern and better authentication technique. Likewise, 71% participants of the control and 83% of the treatment group agreed that the app is using state-of-the-art technique as compared to other existing ones.

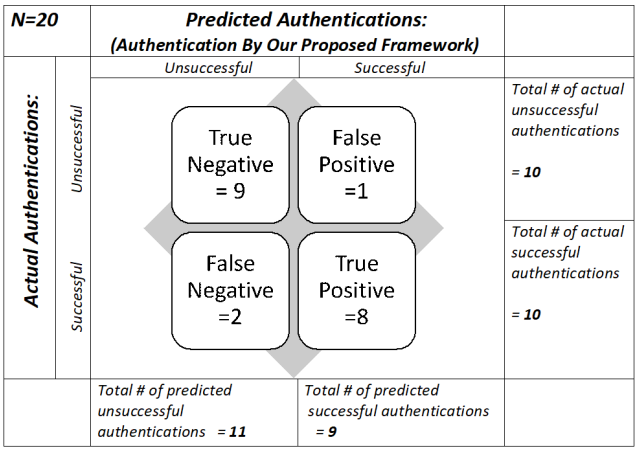


FIGURE 12. Statistics of security measure by confusion matrix.

C. EVALUATION OF SECURITY MEASURE USING CONFUSION MATRIX

The security measure of the proposed technique, being most crucial to examine, was evaluated very carefully using confusion matrix. Total 10 doodle shapes were selected to draw a password for the evaluation of actual and predicted, successful, and unsuccessful authentications. While evaluating any measure or test data using confusion matrix, true values must be known to identify true negative, true positive, false negative, and false positive [29]. Keeping this in mind, the matrix was evaluated by drawing all 10 shapes correctly one time, which means that the proposed technique must authenticate the password 10 times. Also, in those 10 shapes, each one was intentionally drawn wrong for one time to check whether the authentication was denied by the proposed framework or not. The predicted authentications were actually the proposed framework's output, as shown in Fig. 12, Out of 10 actual unsuccessful authentications, the proposed technique denied the authentication for 9 times, which was actually unsuccessful, while only one time a wrong doodle shape was authenticated, i.e., True Negative $= 9$ and False Positive $= 1$, respectively. Similarly, out of 10 successful authentications, two times the authentication was denied to correct doodle shape, (i.e., False Positive $= 2$) and eight times the password was authenticated correctly, which was actually a successful authentication, i.e., True Positive $= 8$.

D. RESULT ANALYSIS

After the comprehensive explanation of results of questionnaire and tasks based survey provided to both control and treatment groups, we are now aimed at describing the comparison of each measure between the control and treatment groups. The usability and usefulness measures were the desired evaluation axes for analysis.

1) USABILITY

The relation of user and system refers to usability. According to ISO 9241-11, usability is the extent to which a product

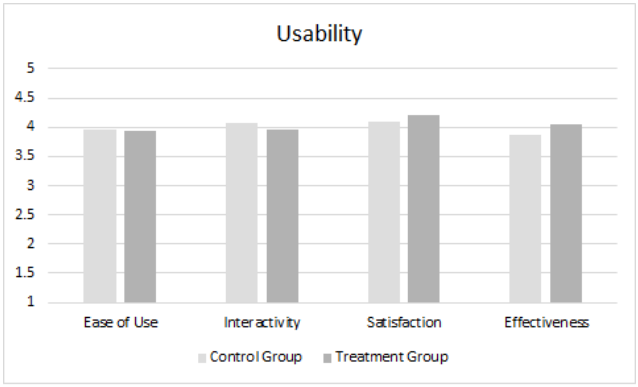


FIGURE 13. Usability average comparison of control and treatment groups.

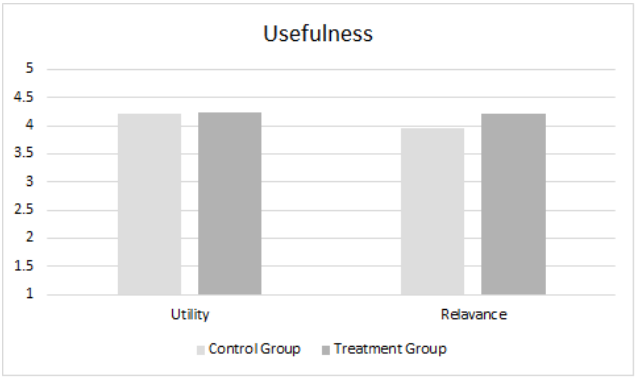


FIGURE 14. Usefulness average comparison of control and treatment groups.

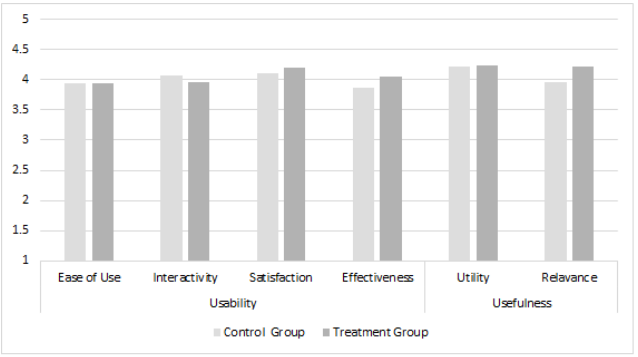


FIGURE 15. Result overview analysis of control and treatment group.

can be used by specified users to achieve a particular goals with effectiveness, efficiency, and satisfaction in a specific context of use. In this research study, four previously mentioned sub-measures were selected for the measurement of usability. Fig. 13 compares the control and treatment groups for usability, where each sub-measure is described in the following subsections.

- **Ease of Use:** The viewpoint of both groups, i.e., control and treatment, lies from neutral to the agreement about the ease of use, as shown in Fig. 13.
- **Interactivity:** Both the groups agreed to the better interactivity with a slight difference, as presented in Fig. 13.
- **Satisfaction:** While analyzing the results, the participants of both groups were found in an agreement with the satisfaction. Fig. 13 depicts the results well.
- **Effectiveness:** The control group lies in the view that is from neutral to agree about the accuracy and timeliness of output, the effectiveness of all functions, and how much a system/app is prone to errors. While the treatment group agrees to the effectiveness of the proposed framework, as described through Fig. 13.

2) USEFULNESS

The measure of usefulness primarily encapsulates the relationship between users and content. It should highlight the relevance of the system for any specific content and test its utility for a specific system or any application while performing an activity that challenges the need and requirements in users' perspective. Fig. 14 compares the control and treatment groups for usefulness and sub-measures utility and relevance.

- **Utility:** The average of both group participants' result shows that both agree to the utility of gesture-based authentication in a 3D space with AR/VR technology, as shown in Fig. 14.
- **Relevance:** The replies graph of control group lies from neutral to agreement about the use of state-of-the-art technology by authentication technique, its contribution to the existing authentication techniques, and better user experience. Whereas the graph of replies of treatment group participants lies from agree to strongly agree, as depicted in Fig. 14.

3) SECURITY

The security of the proposed technique to check for its integrity and successful authorizations was examined by confusion matrix, as described in Fig. 12. The proposed framework successfully identified 9 incorrect passwords and 8 correct passwords out of 10 incorrect and 10 correct passwords, respectively.

E. RESULT OVERVIEW

After a comprehensive discussion about the results of each measure and sub-measure of both control and treatment group, and building a comparison of usability and usefulness of the proposed authentication technique, and an existing authentication technique, we look into the overview of a big picture of all sub-measures and measures, as shown in Fig. 15. The ease of use, interactivity, and satisfaction in usability have almost the same results with a slight differences for both control and treatment group. However, the effectiveness in usability and utility, and relevance in the usefulness of the proposed technique show a dependable result as compared to the existing one. Fig. 15 shows the average results of all sub-measures and compares both control and treatment group.

Abstract results of the security measure are described in Fig. 12. There were 10 actual successful authentications

where the proposed technique gave 9 successful authentications out of which 8 were actually true while 1 was false. On the other hand, there were actual 10 unsuccessful authentications where the proposed technique gave 11 unsuccessful authentications out of which 9 were actually wrong/unsuccessful while 2 were successful authentications.

VII. CONCLUSION

Realizing the need for the integration of modern technologies with authentication schemes, this research proposes a new advancement in the existing authentication techniques by developing an innovative mechanism for authentication. The proposed inventive authentication scheme manipulates augmented reality (AR) with the graphical doodle passwords in a 3D space. The implementation of the proposed framework is such that a user creates a password in a 3D space by pressing the screen of a smartphone and moves it in the 3D space to draw a password. Then the password matching is done by comparing the size and coordinates of the last five drawn doodles. Authentication can only be successful if both the size and coordinates of any set of two doodles match. The evaluation of the proposed technique is based on three measures, i.e., usability, usefulness, and security. Usability and usefulness both are examined through a survey that follows Randomized-Posttest-Only Research design. Participants of the survey were divided into two groups to perform the tasks and then fill in the questionnaire. Further, the results of both groups were compared where the analysis shows that the proposed technique is equally satisfying, easy to use, interactive, and effective as the existing authentication techniques are. Participants also emphasized on the need of more AR based authentication techniques acknowledging the usefulness and utility of them. The security of the proposed technique is evaluated using confusion matrix and on comparing successful and unsuccessful authentications based on predicted and actual authentications can recognize the proposed technique to be secure. Doodle passwords are hard to crack because of a large number of possible doodle shapes and AR being a break-through in the technology can emerge as amusing as well as powerful duo at the same time for authentication schemes. The proposed authentication technique, being the fledgling one, is in its dawning phase of upcoming attempts. In the upcoming phase, more extensive AR schemes will be designed that can be more satisfying, which can fulfil the user expectations.

ACKNOWLEDGMENT

The authors would like to thank the Deanship of Scientific Research, King Saud University for funding through Vice Deanship of Scientific Research Chairs.

REFERENCES

[1] R. G. Rittenhouse, J. A. Chaudry, and M. Lee, "Security in graphical authentication," *Int. J. Secur. Appl.*, vol. 7, no. 3, pp. 347–356, May 2013.

[2] R. T. Azuma, "A survey of augmented reality," *Presence, Teleoperators Virtual Environ.*, vol. 6, no. 4, pp. 355–385, 1997.

[3] D. Schmalstieg and T. Hollerer, *Augmented Reality: Principles and Practice*. London, U.K.: Pearson, 2016. [Online]. Available: https://books.google.com.pk/books?id=qPU2DAAAQBAJ

[4] G. D. Clark and J. Lindqvist, "Engineering gesture–based authentication systems," *IEEE Pervas. Comput.*, vol. 14, no. 1, pp. 18–25, Jan./Mar. 2015.

[5] J. Goldberg, J. Hagman, and V. Sazawal, "Doodling our way to better authentication," in *Proc. ACM Conf. Hum. Factor Comput. Syst. (CHI)*, Apr. 2002.

[6] E. L. Van Den Broek, "Beyond biometrics," *Procedia Comput. Sci.*, vol. 1, no. 1, pp. 2511–2519, 2010.

[7] B. Ducray, "Authentication by gesture recognition: A dynamic biometric application," Ph.D. dissertation, Univ. London, London, U.K., 2017.

[8] A. Almulhem, "A graphical password authentication system," in *Proc. World Congr. Internet Secur. (WorldCIS)*, 2011, pp. 223–225.

[9] R. Dhamija and A. Perrig, "Deja Vu-A user study: Using images for authentication," in *Proc. 9th USENIX Secur. Symp.*, Aug. 2000.

[10] D. Davis, F. Monrose, and M. Reiter, "On user choice in graphical schemes," in *Proc. 13th UNENIX Secur. Symp.*, 2004.

[11] L. Sobrado and J.-C. Birget, "Graphical passwords," *Rutgers Scholar, Electron. Bull. undergraduate Res.*, vol. 4, pp. 12–18, Sep. 2002.

[12] P. B. Maruthi and K. S. Rani, "Recall based authentication system—An overview," in *Proc. Int. Conf. Innov. Appl. Eng. Inf. Technol. (ICIAEIT)*, vol. 3, Mar. 2017.

[13] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effect of tolerance and image choice," in *Proc. 1st Symp. Usable Privacy Secur. (SOUPS)*, Jul. 2005.

[14] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *Int. J. Hum. Comput. Studies*, vol. 63, nos. 1–2, pp. 102–127, 2005.

[15] M. D. H. Abdullah, A. H. Abdullah, N. Ithnin, and H. K. Mammi, "Towards identifying usability and security features of graphical password in knowledge based authentication technique," in *Proc. 2nd Asia Int. Conf. Modelling Simulation (AMS)*, May 2008.

[16] F. A. Alsulaiman and A. El Saddik, "A novel 3D graphical password schema," Multimedia Communication Research Laboratory," in *Proc. IEEE Symp. Virtual Environ., Hum.-Comput. Interfaces Meas. Syst. (VECIMS)*. Ottawa, ON, Canada: Univ. of Ottawa, Jul. 2006, pp. 125–128.

[17] C. Varenhorst, "Passdoodles: A lightweight authentication method," Massachusetts Inst. Technol., Res. Sci. Inst., Cambridge, MA, USA, Jul. 2004.

[18] I. Jermyn and A. Mayer, "The design and analysis of graphical passwords," in *Proc. 8th USENIX Secur. Symp.*, Washington, DC, USA, USA, Aug. 1999.

[19] A. Dennis, B. H. Wixom, and M. R. Roth, *Systems Analysis and Design*, 5th ed. Hoboken, NJ, USA: Wiley, 2018.

[20] A. M. Eljetlawi, "Study and develop a new graphical password system," M.S. thesis, Univ. Technol. Malaysia, Johor Bahru, Malaysia, 2008.

[21] J. Guerra-Casanova, C. Sánchez-Ávila, G. Bailador, and A. de Santos Sierra, "Authentication in mobile devices through hand gesture recognition," *Int. J. Inf. Secur.*, vol. 11, no. 2, pp. 65–83, Apr. 2012.

[22] H. Wang, D. Lymberopoulos, and J. Liu, "Sensor-based user authentication," in *Proc. EWSN*, in Lecture Notes in Computer Science, vol. 8965, T. Abdelzaher, N. Pereira, and E. Tovar, Eds. Heidelberg, Germany: Springer, 2015, pp. 168–185.

[23] M. K. Jain and A. N. Pherwani, "Virtual reality based user authentication system," *Int. J. Sci. Technol. Eng.*, vol. 4, no. 4, pp. 49–53, Oct. 2017.

[24] D. Schafer, "Development and evaluation of authentication schemes for mobile virtual reality," B.S. thesis, Dept. Comput. Sci., Saarland Univ., Saarbrücken, Germany, Mar. 2018. Accessed: Sep. 19, 2019. [Online]. Available: https://umtl.cs.uni-saarland.de/files/thesis_ba_schaefer.pdf

[25] W. Jansen, "Authentication mobile device user through image selection," in *Proc. Data Secur.*, 2004.

[26] D. Lin, P. Dunphy, P. Olivier, and J. Yan, "Graphical passwords and qualitative spatial relation," in *Proc. ACM 3rd Symp. Usable Secur.*, Pittsburgh, PA, USA, Jul. 2007, pp. 161–162.

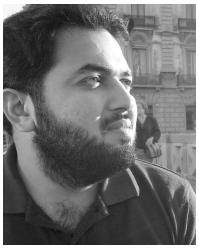
[27] G. Tsakonas, S. Kapidakis, and C. Papatheodorou, "Evaluation of user interaction in digital libraries," in *Proc. DELOS WP7 Workshop Eval. Digit. Libraries*, Padua, Italy, 2004.

[28] N. Fuhr, G. Tsakonas, T. Aalberg, M. Agosti, P. Hansen, S. Kapidakis, C. Klas, L. Kovacs, M. Landoni, and A. Micsik, "Evaluation of digital libraries," *Int. J. Digit. Libraries*, vol. 8, no. 1, pp. 21–38, 2007.

[29] S. Visa, B. Ramsay, A. Ralescu, and E. Van Der Knaap, "Confusion matrix-based feature selection," in *Proc. CEUR Workshop*, vol. 710, 2011, pp. 120–127.

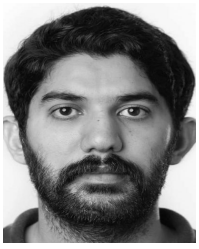
[30] J. Fraenkel and N. Wallen, *How to Design and Evaluate Research in Education*. New York, NY, USA: McGraw-Hill, 2008.
[31] P. H. Rossi, M. W. Lipsey, and H. E. Freeman, *Evaluation: A Systematic Approach*, 7th ed. Newbury Park, CA, USA: Sage,, 2003.
[32] T. Novoda. (2018). *Getting Started With Google Arcore on Android*. [Online]. Available: https://blog.novoda.com/getting-started-with-google-arcore-on-android/
[33] S. Ratnottar. (2019). *Augmented Reality (AR) Trends: The Past, Present Future Predictions for 2019*. [Online]. Available: https://towardsdatascience.com/augmented-reality-ar-trends-the-past-present-future-predictions-for-2019-8e1148345304
[34] G. C. Lab. *AR Drawing*. Accessed: Sep. 13, 2019. [Online]. Available: https://github.com/googlecreativelab/ar-drawing-java
[35] M. A. Khan, I. Ud Din, S. U. Jadoon, M. K. Khan, M. Guizani, and K. A. Awan, "g-RATl A novel graphical randomized authentication technique for consumer smart devices," *IEEE Trans. Consum. Electron.*, vol. 65, no. 2, pp. 215–223, May 2019.
[36] C. Hung, Y. Fanjiang, K. Chung, and C. Kao, "A door lock system with augmented reality technology," in *Proc. IEEE 6th Global Conf. Consum. Electron. (GCCE)*, Nagoya, Japan, Oct. 2017, pp. 1–2, doi: 10.1109/GCCE.2017.8229462.
[37] D. Balfanz, G. Durfee, D. K. Smetters, and R. E. Grinter, "In search of usable security: Five lessons from the field," *IEEE Security Privacy*, vol. 2, no. 5, pp. 19–24, Oct. 2004.
[38] A. Ometov, S. V. Bezzateev, J. Kannisto, J. Harju, S. Andreev, and Y. Koucheryavy, "Facilitating the delegation of use for private devices in the era of the Internet of wearable things," *IEEE Internet Things J.*, vol. 4, no. 4, pp. 843–854, Aug. 2017.
[39] D. Jo and G. J. Kim, "ARIoT: Scalable augmented reality framework for interacting with Internet of Things appliances everywhere," *IEEE Trans. Consum. Electron.*, vol. 62, no. 3, pp. 334–340, Aug. 2016.
[40] M. F. Alam, S. Katsikas, O. Beltramello, and S. Hadjiefthymiades, "Augmented and virtual reality based monitoring and safety system: A prototype IoT platform," *J. Netw. Comput. Appl.*, vol. 89, pp. 109–119, Jul. 2017.
[41] A. Manzoor, M. A. Shah, H. A. Khattak, I. U. Din, and M. K. Khan, "Multi-tier authentication schemes for fog computing: Architecture, security perspective, and challenges," *Int. J. Commun. Syst.*, p. e4033, Jun. 2019.

WAQAS WAZIR received the bachelor's degree in security and authentication from IMSciences Peshawar. He is currently pursuing the M.S. degree in computer science with the Department of Computer Science, COMSATS University Islamabad, Pakistan. He is also an part-time freelancer, developing Android-based applications. His research interests include the Internet of Things, augmented reality, authentication, and network authentication.



HASAN ALI KHATTAK (Senior Member, IEEE) received the B.S. degree in computer science from the University of Peshawar, Peshawar, Pakistan, in 2006, the master's degree in information engineering from Politecnico di Torino, Torino, Italy, in 2011, and the Ph.D. degree in electrical and computer engineering from Politecnico di Bari, Bari, Italy, in April 2015. He has been an Assistant Professor of computer science, since January 2016. His current research interests include Web of Things, data sciences, and social engineering for future smart cities. His perspective research areas are the application of machine learning and data sciences for improving and enhancing quality of life in smart urban spaces through predictive analysis and visualization. He is an active member of the IEEE ComSoc, IEEE VTS, and Internet Society. Along with publishing in good research venues and completing successful funded National and International funded projects, he is also serving as a reviewer in reputed venues, such as IEEE Access, *IEEE Network Magazine, IEEE Consumer Electronics, Hindawi, SAI, IET,* and a few national publishers. He is currently involved in several funded research projects in various domains, such as semantic Web of Things and fog computing while exploring ontologies and Web technologies using Contiki OS, NS 2/3, and Omnet++ frameworks.

AHMAD ALMOGREN (Senior Member, IEEE) received the Ph.D. degree in computer science from Southern Methodist University, Dallas, TX, USA, in 2002. He was an Assistant Professor of computer science and a member of the Scientific Council with the Riyadh College of Technology. He also served as the Dean of the College of Computer and Information Sciences and the Head of the Council of Academic, Al-Yamamah University. He is currently a Professor and the Vice Dean for the development and quality with the College of Computer and Information Sciences, King Saud University. His research interests include mobile and pervasive computing, cyber security, and computer networks. He has served as a Guest Editor at several computer journals.



MUDASSAR ALI KHAN received the master's degree from the Department of Computer Science, Quaid-i-Azam University, Islamabad. He is currently working as a Lecturer with the Department of Information Technology, The University of Haripur, Pakistan. His recent undergraduate research supervisions include vehicle owner authentication based on hand gesture recognition, sentiment analysis of news articles, and Twitter feeds detecting biasness in expressions. Besides, he has been working over digital multimedia creation and manipulation with a company MASH, Peshawar. His research interests include usable security, information management and retrieval, and computer-aided intelligence.

IKRAM UD DIN (Senior Member, IEEE) received the M.Sc. degree in computer science and the M.S. degree in computer networking from the Department of Computer Science, University of Peshawar, Pakistan, and the Ph.D. degree in computer science from the School of Computing, Universiti Utara Malaysia (UUM). He served as an IEEE UUM Student Branch Professional Chair. He has more than ten years of teaching and research experience in different universities/organizations. He is currently working as a Lecturer with the Department of Information Technology, The University of Haripur. His current research interests include traffic measurement and analysis for monitoring quality of service, mobility and cache management in information-centric networking, and the Internet of Things.