Surveying Research on Biometric Authentication Methods in Computer-Simulated Reality

Brian Lasher
UCF College of Engineering & Computer Science
University of Central Florida
Orlando, FL, USA
brian.lasher@knights.ucf.edu

John Mulloor
UCF College of Engineering & Computer Science
University of Central Florida
Orlando, FL, USA
john.mulloor@knights.ucf.edu

Zachary Russell
UCF College of Engineering & Computer Science
University of Central Florida
Orlando, FL, USA
zachrussell17@knights.ucf.edu

ABSTRACT

The computer-simulated reality market – including Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR) – has begun to grow rapidly over the preceding years and has slowly become a serious contender for use by the general population in our everyday lives. Garnering promising investments from large companies like Facebook (Meta), Microsoft, and Google, computer-simulated reality is moving to a widely-adaptable market that is starting to intertwine with e-commerce and massively multiplayer online interactions. With growing popularity, it is important the security of the computer-simulated reality devices are evaluated, specifically their authentication methods. These devices store and access sensitive information continuously while they are in use. In order for these devices to become widely-adopted, they need to have proper authentication methods to prevent malicious attacks from stealing sensitive data collected by these devices. The biometric authentication methods gathered offer a potential alternative to current authentication methods found in common devices now. Thus, offering a way to secure VR/AR/MR devices so that computer-simulated technology can expand into more markets.

CCS CONCEPTS

• Security and Privacy → Security Service → Authentication → Biometric → Human-centered Computing → Human Computer Interaction → Interaction Paradigms → Virtual Reality

KEYWORDS

Metaverse, augmented reality, virtual reality, mixed reality, biometrics, security, computer science, voice recognition, authentication, computer-simulated reality,

1 INTRODUCTION

With the rate of advancements in VR, AR, and MR, it is only a matter of time before these technologies play a role in our everyday lives. In 2021, the global market size for computer-simulated reality technology was valued at USD 21.83 billion [7]. This global market value is expected to grow rapidly and garner even more popularity from different types of potential markets. Not only is the average consumer heavily interested in the latest VR technologies, but also other sectors of the market including Aerospace & Defense, Enterprise, and Healthcare as pictured in Figure 1.

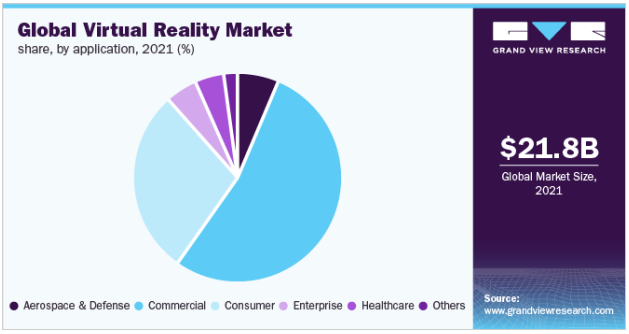

Figure 1: VR Market share by application [7]

By peering into where computer-simulated reality devices could find themselves over the next 10 years, this begs the question: do these devices have proper security integrated into them? These devices contain different sensors and functionality that can collect sensitive information pertaining to the current user. In cases of personal use, this threat to potentially important information is less severe, however in a use-case of the healthcare, retail, or defense industry, these devices need to be as secure as possible. The leak of patient information, defense secrets, or payment information is data that needs to be properly secured in these devices.

The lack of authentication mechanisms in current computer-simulated devices is worrisome in a field that wants to advance this technology to e-commerce and other important sectors. These devices could add a weak point to the attack surface of many large companies, hence why it is important that proper security is in these devices.

The survey begins by evaluating where the current security of computer-simulated reality devices stand and discussing their security issues. The technique for obtaining and analyzing relevant research is discussed in section 3. The evaluation of the survey results is outlined in section 4. Following the evaluation, is a discussion of the implications biometric security could have on the computer-simulated reality field. Our survey of research concludes in section 6.

2 PROBLEM STATEMENT

With the computer-simulated reality industry looking to grow into widespread massively multiplayer online interactions and pushing for a role in the e-commerce industry, it is important to assess whether these technologies are secure enough for these endeavors. Computer-simulated reality devices require access to a range of sensitive data including your GPS location and accelerometer/gyroscopic sensors in the headset or mobile device. These devices lack secure authentication methods to ensure no one can take your device and impersonate you. This survey analyzes a possible solution to these issues with an exploration into both initial and continuous biometric authentication for computer-simulated reality devices. Biometric authentication offers the possibility of a secure computer-simulated reality environment where a user can keep their identity, personal information, and devices safe from any malicious adversaries aiming to take advantage of them.

3 APPROACH

To conduct our survey of research, it is important a clear and concise method is used to collect research, filter it, evaluate it, and draw conclusions. So-Hui Park et. al [6] heavily inspired our survey technique as outlined in Figure 2.

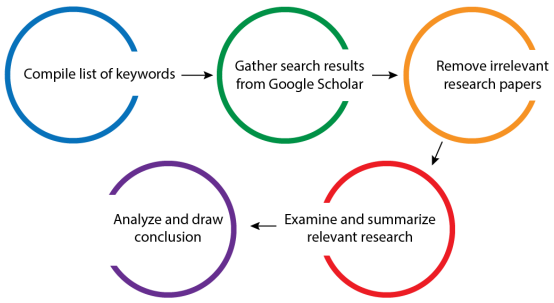

Figure 2: Technical method used by the survey team

To examine the greatest number of research papers, while ensuring we are only reading ones relevant to the survey's goal, a method of searching and filtering was devised. Specific keywords were used in Google Scholar to return the highest amount of relevant research papers. The keywords used and total results returned is described in Figure 3.

Initial Keyword	Additional Keywords	# of returned results	# of results selected
Virtual Reality	biometrics	26,300	5
	authentication	73,300	3
	biometric authentication	16,500	8
Augmented Reality	biometrics	21,700	2
	authentication	38,500	5
	biometric authentication	6,740	10
Total:		183,040	33

Figure 3: Above table depicts the keywords, returned results, and usable results from Google Scholar from the following keywords

3.1 Filtering Research

Once we compiled all of the possible research papers returned from Google Scholar, we began sorting the research and removed any papers that were deemed irrelevant to our survey goals. The total number of papers after filtering are outlined in the *Total* row in Figure 3. The team used three questions to determine whether a research paper was relevant to the survey:

1. Does the research paper relate to computer-simulated reality?
2. Does the research paper focus on security topics related to computer-simulated reality?
3. Is the security topic related to user authentication?
4. Is the authentication procedure specifically biometric authentication?

If all 4 questions were fulfilled, then the research paper was deemed relevant to the survey and added to the list of papers to analyze. If all 4 questions were not met, then the paper was removed from the survey. It is worth noting that biometric authentication encompasses using any part of a human's biological makeup that can be used to authenticate a user including voice recognition, retinal scanning, kinesiological movements, fingerprint scanning, and facial recognition. The total number of results selected after filtering was 33, however after deciding which results were duplicates, the final total was narrowed down to 23 papers.

3.2 Research Examination

With a final collection of relevant papers, each paper then had to be examined and summarized. To efficiently grasp the concept of each paper and the relevance it provided, key portions from the paper were used to summarize and evaluate it:

1. Attack Model
2. Authentication Model
3. Issues and Exploits
4. Methods
5. Results

The authentication method's attack model was first taken into consideration and evaluated against the other papers. The less the adversary has access to and the less known information they have about the authentication mechanism or device, the better the attack model. The authentication model was evaluated on it having the best challenge-response structure; meaning the authentication method with the hardest challenge for the adversary to produce a response was evaluated higher than other mechanisms with easier challenges for the adversary to produce a response. The issues each research team ran into were incorporated into the evaluation because these issues could be possible weak points for exposing vulnerabilities. These issues also could lead to challenges if the authentication mechanism were to be implemented across the computer-simulated reality field. The method of testing the authentication mechanism needed to be thorough and sound in order to display the mechanism works reliably in all use-cases; the more effective the authentication method, the better outlook it provided on its implementation into the computer-simulated reality field. Each authentication method's error rate and false succession rate was evaluated to determine its effectiveness. Where the false rejection rate (FRR) is the rate at which the authentication method fails to authenticate a valid user, and the false acceptance rate (FAR) is the rate at which the authentication method does authenticate an invalid user.

3.3 Research Analysis

Analysis was carried out in order to draw conclusions pertaining to the key idea of our survey. Based on previous criteria outlined in section 3.2, each paper was rated on their effectiveness and secureness of their biometric authentication method in computer-simulated reality devices. Each authentication mechanism was both compared against each other, and compared against the current authentication mechanisms available to VR/AR/MR devices now. It is important to note that not all of the papers evaluated aimed to create an authentication method to serve the purpose of securing computer-simulated reality devices. Some of the papers designed malicious tools to attack aspects of these devices, and then offered possible countermeasures using biometrics; while others designed biometric authentication methods to protect against an attack model they created. One category of papers worked to highlight the vulnerabilities of these devices, while the other devised authentication methods to secure them, but both types of papers aid our survey. Specific evaluations of the best performing authentication methods are discussed in section 4.

4 EVALUATION

Consumers need to be informed about the data being collected by VR/AR/MR devices and how it can be used from an adversarial perspective. Computer-simulated reality devices are so intertwined with the human user it opens the possibility of new security issues. In the case of VR and AR devices, the human and device work in symbiosis with one another. To function properly and be secure, the device needs to know information about the wearer and their environment. VR/AR/MR devices require unprecedented access to a user's environment in order for them to operate in conjunction with the user. These devices need to utilize cameras, gyroscopes, accelerometers, magnetometers, LiDAR, and other external environment measuring sensors. With all of these sensors, it grants computer-simulated devices unprecedented access to both the user and their entire environment.

4.1 Vulnerabilities of the Metaverse

The Metaverse carries differences from current technology not yet explored, however, like current technology, computer-simulated devices take part in mass data collection through physical devices and software. Like any other device, application, or software, the Metaverse gathers personal information like user's name, address, birthdate, height, weight, sex, and other needed personally identifiable information (PII). The dangers of the virtual world can reveal other information like behavioral actions or physiological aspects of a user [8].

With applications and devices that take advantage of VR, AR, and MR devices, there are new risks introduced that need to be secured. In order for these devices to function and act properly, these devices need to know the relative location and motion of the user's head and body. This information is found through the usage of multiple motion-based sensors, which together form the inertial measurement unit data (IMU) [14]. Other sensors, such as cameras, microphones, and fingerprint scanners, can be used to capture information about a user's face, fingerprint, eye, keystrokes, touch gestures, voice, motions, and more [4]. All of the readings gathered from these sensors are able to map and yield accurate user movements to enhance the virtual experience. It is important to point out that with the use of these virtual world devices and biometric information they gather, it is possible to interpret the user's facial muscle patterns, gender, ethnic identity, speech content, and bone-born vibrations[1]. Furthermore, the IMU can be used to make inferences about the wearer to reveal personal information related to their kinesiological actions while using the device.

With the use of AR devices, time-stamped information of a users' activities, locations that a user may have visited, and even the environments that the headset has regenerated in the device can be uncovered [5]. Cameras within AR devices could be tampered with and allow adversaries to unjustly spy on their victims. The collection of other biometric information, like eye tracking data and iris reading, create completely new and different problems. With the use of iris scanners, it is possible for adversaries with access to only one frame of a user's iris to

impersonate and hold the identity of another individual [3]. This iris scan could even be used to even gain access to personal identifiable information, physical assets, and other areas of value.

To emphasize the importance of securing these computer-simulated reality devices, researchers have begun to showcase AR/VR headset attacks. One such test, labeled Face-Mic, focused on attacking zero-permission motion sensors to capture a user's speech and PII. Microphones require explicit use permission from the user, whereas motion sensors do not since they are a primary sensor needed for computer-simulated reality devices to function. The attack used the motion sensor to capture facial muscle movements and bone-born vibrations; which was then used to extract a user's gender, identification, and speech by examining the relationship between bone-borne vibrations/facial movements and speech [1]. The storing and handling of biometric information related to the user calls for security mechanisms to be in place to protect this data from being exploited by adversaries.

4.2 Authentication Mechanisms

Authentication mechanisms need to evolve with the industry, meaning passwords and PIN numbers will no longer be the most efficient and secure when discussing virtual, augmented, and mixed-reality equipment devices. Researchers have pinpointed biometric data as a possibility to creating a secure metaverse. However, there are still several challenges to overcome in order to make biometric authentication accurate, yet secure.

Behavioral and physiological aspects of an individual are not typically shared on a day to day basis in the current landscape of technology. Thus, there is a great need for authentication, especially in sectors where this technology is used to help the public sector. For now, virtual, mixed, and augmented reality systems are being used for individual means, for either personal or commercial use. Personal usage systems, such as Meta Quest 2, have little to no security measures or authentication mechanisms. This practice is not wise and is of great concern for the future, as these devices make their way into sectors with a higher risk for exploitation. For example, when VR/AR use becomes widespread in the healthcare and defense industries, there will be an urgency for better authentication due to the highly sensitive information these industries have access to. When VR/AR/MR devices become involved in handling sensitive data there will be a clear increase in interest by malicious actors. As of now, research shows that the current authentication measures being applied to non-VR/AR/MR systems are being applied to the VR/AR/MR devices [9]. Researchers have tried to explain how these solutions are the way to a secure future, but there is great opposition to these sentiments.

In a virtual reality context, users would use their controllers, joysticks, and buttons to manipulate the environment and enter a password. Virtual reality headsets do not use a physical keyboard as a part of their peripheral make-up. Thus, with the use of passwords in a virtual world context, there may be an increase of less-complex, easy-to-guess passwords. Long, confusing passwords will take exponentially longer to type in without the use of a physical keyboard, leading to a negative impact on user experience. Thus resulting in the use of easy, quick-to-guess passwords and PIN numbers. Overall, the PIN number and password approach is not secure enough and there is a great need for stronger and more accurate solutions in order to protect a user's sensitive data in the computer-simulated reality environment.

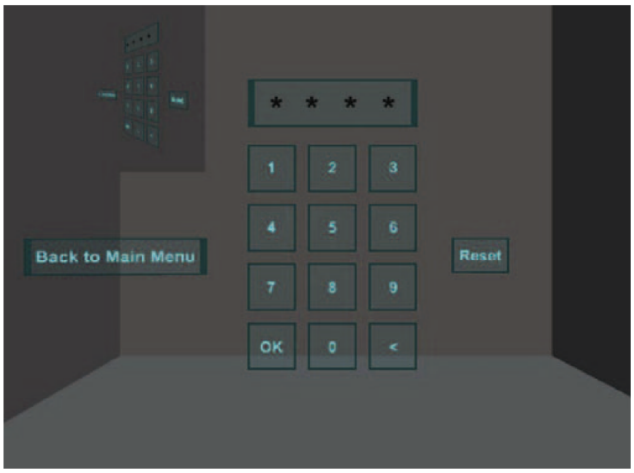

Figure 4: Current Mechanisms in Place to Authenticate in Virtual Reality

Due to the lack of current solutions, this topic of new authentication mechanisms has been a major topic for research. The key to a prosperous and secure future within the virtual space, that is the Metaverse, is the use of biometric authentication on all devices used to access the virtual environment. By using biometric verification, users are able to be consistently, accurately, and constantly authenticate, something that cannot be offered by the present solutions of password/PIN authentication.

4.2.1 Bone Conduction Authentication - Bone conduction can be described as the transmission of the propagation of waves through bone tissue. Authentication using bone conduction would occur by cross-checking a past conduction baseline with the user's current result [10]. The accuracy of this authentication method is reliant on the specific bone that is used. A proposed solution by researchers would be to broadcast audio through a bone conduction speaker, where the signal would change once it passes through one's head. Specific characteristics of the wearer, like their body tissues, cartilage, fluids, and their fluid's location, would reveal who the wearer is, and if they are authenticated to use the device. In some early tests of bone conduction as a means of authentication, researchers found that proper authentication took place 97% of the time, for both the measures of identification and authentication [11].

However, the technology for bone conduction authentication may need improvement as during many of these experiments, test subjects were in rooms without background noise, meaning

signals were not impacted at all [11]. Another key area of concern in this study, is the relatively high rates of false positives and negatives. The FRR measured was 6.9% and the FAR measured was also 6.9% in this study[11]. In another study, where bone conduction authentication was conducted on the wrist, both FAR and FRR were approximately 0.7% [10].

From these results, conclusions can be made that the wrist authentication mechanism is more reliable, but many companies have stated that VR/MR/AR is looking to evolve in terms of hardware. The evolution of the computer-simulated reality devices will lead to a space where less physical device mechanisms are optimal. Thus, in order to attain these better metrics, there is a need for more sensors and physical hardware. Therefore, there is a key need for research into the field and further experiments on skull-based bone conduction techniques in order to get these false negative and positive rates down. However besides these challenges, the past and present research shows that authentication via interpreting bone conduction produces promising results for authentication for devices that require headsets.

From a security perspective, bone conduction readings must be made private and secure. If adversaries were able to gain access to records containing user's bone conduction readings, then there is concern that the manipulation of these signals could take place in order to benefit the adversary. Having access to a user's bone conduction readings benefits the adversary in cases where they are attempting to access a user's system or determine PII information about the user.

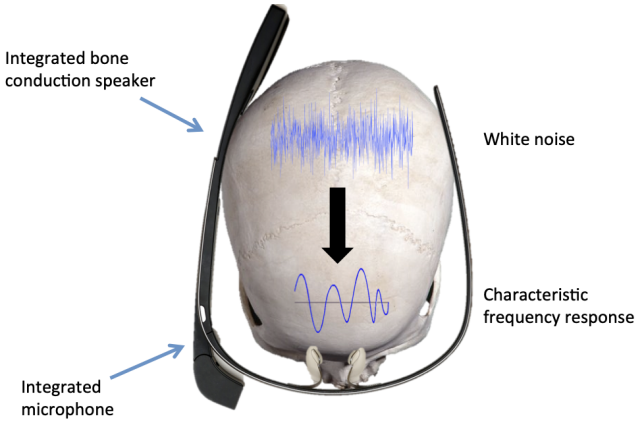

Figure 5: Bone Conduction Mechanism is described as audio is transmitted from the front of the skull to back - Referenced from [11]: "SkullConduct: Biometric User Identification on Eyewear Computers Using Bone Conduction Through the Skull"

In order to limit these occurrences, researchers have stated that noise must be added to readings found on these sensors to mitigate listening attacks. In these attacks adversaries can employ viruses or malware to hack into these sensors and broadcast their readings. By adding noise to the bone conduction data before it is stored, the data would essentially be scrambled, decreasing the probability that leaked data could be used to employ an attack on the user's system or information. Researchers suggested adding padding of a higher density in order to absorb more vibrations, thus resulting in a greater challenge for the adversary to read the user's bone conduction profile while they are using the device [1].

4.2.2 Optic Based Authentication - The eyes, specifically the retina and iris, can be used to authenticate individuals. Since cameras are involved and needed with AR technology, this solution seems to be very plausible and realistic, as the equipment could be leveraged for both functionality and security. In terms of retinal scanning, the authentication method is largely based on reading the blood vessel pattern within the eyes [12]. Like a fingerprint, the blood vessel formation in a pair of eyes is unique to every person. To perform a retinal scan, a picture is taken with a fundus camera. Then, features from the image are extracted and compared with features from past scans. One team was able to produce retinal scans that achieved an accuracy of 99% and an FAR and FRR of 0.006%[22].

Iris scanning is another optic-based authentication method that offers an alternative to retinal scanning. In this approach, an infrared imaging system is used to capture a scan of the user's iris. However, to perform a scan and analyze an iris image, the eye needs to be in a perfect alignment in order that the specific characteristics of the eye can be captured for analysis and processing. Once in this position, the device takes an image and begins analysis and matching of its characteristics, including the iris pattern [13]. One research studying the classification of iris images using a hybrid of Fourier transformations with Bernstein polynomials yielded promising results. Their hybrid classification algorithm produced an accuracy of 97% with an FAR of $\leq 0.5\%$ and an FRR of $\leq 0.6\%$[21]. In terms of usability in the computer-simulated reality field, other research has concluded that images of irises as low as 50-60 pixels in size can yield a 90% recognition rate [3]. Thus, from an authentication perspective, the use of eyes through either retinal or iris scanning is a very effective and accurate mechanism even using poor image quality. Which could prove to be beneficial if the quality of imaging inside VR/AR/MR headsets are poor.

In order for retinal scans to be used, there is a need for a fundus camera, which can be costly. This is important to take into account as the production of these AR or VR devices may not already support this type of camera technology. Another challenge iris scanning faces is the need for the eye to be very close to the camera. This challenge may impact how and future devices are designed to incorporate iris scanning as an authentication method. Overall, from a functionality standpoint, iris scanning may be a more plausible solution to biometric authentication for the next generation of computer-simulated reality devices. From a security perspective, it is important to understand that these images of irises and retinas can be stolen and used to bypass authentication mechanisms. Thus, it is important, if iris scanning is chosen as the methodology, that these images are protected and held private. Researchers suggested using filters to reduce the quality of the scans and frames of the iris. This practice would be used to stop the clear capturing of images of the iris by adversaries, however

the quality of the iris image needs to remain at a high enough level to maintain an efficient enough authentication success rate for iris scanning to be viable[3].

4.2.3 Kinesiological Authentication - Kinesiological movements are mechanical body movements unique to individuals. With the help of machine learning algorithms, user verification from kinesiological movements can be used to verify users in computer-simulated reality environments[2]. Motion and gait-based authentication mechanisms provide a key advantage to its wearer, as there is no active, explicit action a user needs to perform. Authentication can be observed by devices through the regular movement and walking of an individual. In current authentication implementations, like the use of PIN numbers and passwords, explicit user input is needed to validate a user. With this mechanism, an opportunity arises of innate, continuous authentication with no explicit user inputs.

This authentication mechanism can be achieved by a variety of ways using cameras, radio signals, floor sensors, and wearable sensors [15]. VR/AR/MR devices would utilize their wearable sensors in the headset and controllers. With the sensors in the headset devices, the gyroscopes and accelerometers would be able to measure the movements in an individual's pace and step. Researchers in one study have found that gait-based authentication mechanisms have a 97.3% recognition accuracy and a 3.5% equal error rate (EER) in smart-watch technology, and these percentages can be improved with better technology and more research [15]. Due to the overlap in sensors and other information reading systems, these authentication mechanisms can be applied to computer-simulated reality devices. Another great benefit to this implementation involves the consistency of the placement of the device. Based on the architecture and design of most computer-generated reality devices, there is always a headset component. Thus, the orientation and placement of the sensors would not be impacted from time to time, as these two factors remain constant across computer-simulated reality devices[15].

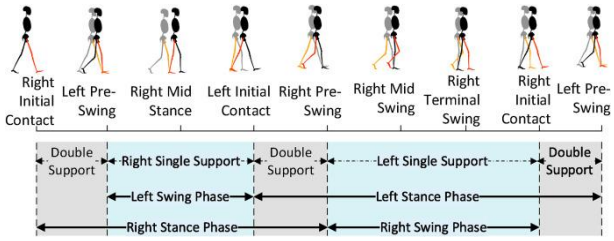

Figure 6: The types of data that can be taken from the sensors in wearable technology and applied to authenticate users - Referenced from [16]: "GaitCode: Gait-based continuous authentication using multimodal learning and wearable sensors"

Possible challenges to the implementation of the motion and gait-based biometric verification mechanism include the need for an individual to move for a reading to take place [5]. Furthermore, if continuous authentication using kinesiological movements is desired, then activities performed while wearing VR/AR/MR devices must include the movement of the user. Gait and motion-based sensors require an individual to be mobile and have the ability to walk and move. Thus, this solution is not accessible for all individuals who desire to use VR/AR/MR devices [5]. The variability of height and weight across users is another drawback kinesiological authentication faces [5]. With changes in these factors, sensor readings may be impacted and fail to provide clear and concise authentication. Thus, it is recommended that motion-based authentication mechanisms be a complementary authentication measure in conjunction with another method simultaneously.

4.2.4 Voice and Touch-Based Authentication - Voice and touch-based authentication mechanisms provide another alternative to protect individuals' sensitive data. Touch-based authentication through the use of fingerprint scanning and other mechanisms has seen widespread adoption among devices like smartphones, personal computers, and desktop computers. In previous studies, the false acceptance rate of an individual was 0.01%, and the false rejection rate was 1.4% [17].

Other types of touch-based authentication have been proposed, such as the analysis of an individual's touch patterns. In another study, research was conducted on touch-based gesture biometric authentication mechanisms for mobile devices. The touch gestures consisted of different patterns either generated by users or commonly used ones set by the experiment, and these gestures were performed on a touch screen with no fingerprint sensors. Thus, touch patterns were analyzed only. On average, there was a false negative and positive rate of about 4.9% for all gestures, which can also be referred to as the equal error rate [20]. Therefore, it can be understood that in terms of authentication performance, there is a drop off in false negatives and positives, when looking at touch pattern analysis as a means for authentication. Thus, fingerprint scanning is an accurate, scalable, proven, and realistic mechanism for biometric authentication on all types of devices, including VR/MR/AR devices. Thus, the addition of touch-based scanners would provide a great benefit for the security of this new platform.

In terms of voice-based authentication, this mechanism would work similarly to fingerprint analysis, where certain characteristics of an individual's voice are extracted and used to identify them. Recently there have been studies to use voice as a means of authentication, providing continuous authentication. In one such study, virtual assistants, like Google Home, Siri, and Alexa, were looked at in order to secure them. To secure them, a solution of voice authentication was brought up in order to restrict the openness of the method. In this research study was tested with a variety of languages, a 97% accuracy was found, along with a less than 0.1% false positive rate. Within this study, the false negative rate was not made known, but said to be less than 5% [23]. These principles, applied to virtual assistants, can be used in the computer-simulated reality sector, as microphones are used as a key tool in this analysis. However, the notion that speech and

voice can be a reliable method of showing uniqueness from individual to individual has been challenged by researchers.

Scientists have explained that the utilization of recording devices and the methodology of speech analysis cannot be used to uniquely identify individuals. It has been demonstrated that individual's voices can change over time and some individuals have the ability to voluntarily alter and disguise their voices [18]. Furthermore, voice-based authentication requires an optimal environment for measurement; an environment unfit for voice-based authentication can impact the accuracy of the authentication system. Researchers also argue that the quality of sound from a speech sample may be impacted with the usage of a microphone that cannot be regulated by the overall system [18]. In the case of virtual, augmented, or mixed reality, this would not be an issue, unless a user utilizes an external microphone instead of the built-in microphone provided by the device. Other possible complications include illness. A user that contracts a voice-altering illness would prove to be challenging for voice-based authentication because the characteristics of the user's voice changes on a short timeline. Minding the challenges, speech and voice recognition is recognized as another area of future research that can be made into a reliable authentication mechanism. Researchers have begun to draw awareness to voices and speech pattern analysis, as machine learning developments could be leveraged to provide identification, validation, and authentication of users for the future[5].

5 DISCUSSION

From the evaluated biometric authentication methods, each with their positives and negatives, it is important to evaluate them against both each other and current authentication methods in use by computer-simulated reality devices today.

5.1 Potential For Research/Attackers

It is worth discussing the creativity of both authentication methods and attack patterns associated with the use of biometrics. We found using bone conduction as a means for authentication to be a novel idea, which sparked the discussion of how many developing authentication methods can spring out of developer and engineer creativity. With that said, adversaries also employ their creativity to find new ways to manipulate the sensors found in headsets for malicious purposes. The aforementioned Face-Mic attack was of concern to us, notably because it uses an attack vector that is difficult to prepare for. Adversaries can and will exploit anything available to them in order to achieve their goals. With the wide variety of sensors used in AR/VR/MR headsets, the principle of easiest penetration is a cause of concern. A typical user setup has many sensors which all pose as windows of opportunities for hackers to exploit.

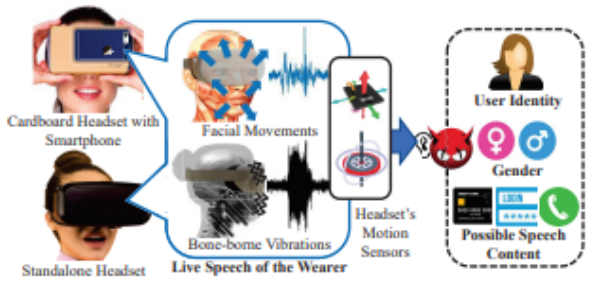

Figure 7: Image depiction of the Face-Mic attack - referenced from [1]: "Face-Mic: inferring live speech and speaker identity via subtle facial dynamics captured by AR/VR motion sensors"

5.2 Application of Best Practices

It is imperative for developers and engineers to apply existing best practices in regards to cybersecurity. The violation of simple practices can cause immense damage to affected parties. As an example, we present the recent biometric data breach of Biostar 2, a security platform owned by Suprema used to authenticate employees. The biometric data breach occurred in 2019, with 28 million records of 1 million unique users around the world found vulnerable [19]. Researchers uncovered extremely sensitive information such as facial photos, fingerprints, unencrypted usernames and passwords, and staff data. In addition, these researchers were able to manipulate records by adding new data or modifying existing data. The data was found because the biometric information was stored largely unencrypted and unsecured. Best practices, such as hashing or encrypting the records in the database and securing the database itself, should have already been in place to prevent this breach. In addition, companies should be ready to quickly patch security vulnerabilities and bugs that will no doubt arise.

5.3 Unchangeability of Biometric Data

The exponential issues caused by the breach of biometric information needs to be included in the discussion of using biometric authentication methods. Biometric information, once exposed, cannot be changed in the same fashion that a stolen username and/or password can. Once an adversary has a user's biometrics, they will forever have that user's sensitive identification information. This poses extreme pressure on companies to properly handle biometric data records in secure storage. In addition, users should exercise caution and judgment before sharing biometrics with any party. The data shared must satisfy a need, and alternatives should be explored before having to share biometric authentication. Users also need to verify the reputability of the receiver in order to ensure that their data will be safe from any adversaries. This aspect also comes down to user's doing their own due diligence; user's need to be educated on how to avoid common attacks like phishing that could result in them sending their biometric information to unreputable sources.

5.4 Variance of Results Across Research

During our survey, our team evaluated and analyzed a range of different authentication methods that produced varying results, but aimed to achieve the same goal. The specific sources discussed in this survey have multiple equally important counterparts that produced varying, yet similar results. This variance is produced by the particular method, technology, or algorithm these research teams employed. As an example, there are multiple studies of authentication using the iris of the eye. Each of these studies produce varying accuracy rates, false acceptance rates, and false rejection rates. Although this is one example from our survey, the team observed this across many of the different authentication methods that involved multiple paths to the same goal. Therefore, we cannot conclude the efficiency of one singular authentication method discussed in this survey, because there are so many studies similar to it. The best our survey aims to do is evaluate each biometric-focused authentication subset and determine an overall outlook on the specific technology and its use in the computer-simulated reality field.

5.5 Comparison of Authentication Methods

Table 5.5.1 in the appendix displays a comparison of the biometric authentication mechanisms only presented in this paper. Our evaluation metrics include accuracy, false acceptance rate, false rejection rate, usability, security risk mitigation technique(s), and any additional notes deemed significant for comparison. As we stated in section 5.4, the metrics shown in table 5.5.1 do not reflect all authentication method variants for each subset of biometric authentication.

5.6 Omitted Authentication Methods

After the application of our survey methods, our group has analyzed five methods of biometric authentication that could be used in AR/VR/MR headsets. It is important to discuss that these are not the only authentication methods available; however, we deemed them to be the most feasible for use in computer-simulated reality headsets. Omitted authentication methods that were researched include:

- Keystroke Recognition
- Signature Recognition
- DNA Recognition

Keystroke recognition was omitted by our team due to the impracticality of requiring an extra peripheral by the user. Requiring additional physical equipment for the express purpose of authentication did not make sense for a computer-simulated reality device and could negatively affect the user experience. Our team decided to omit signature recognition as a potential authentication method because it is easily victimized by listening attacks and has the potential for lazy users to produce easily identifiable signatures. Adversaries employing malware to the device could easily gather data during authentication and replicate the user's signature. DNA based authentication was omitted from our survey due to its expensive costs associated with providing the needed equipment for verification into computer-simulated reality devices.

6 WORK DISTRIBUTION

As a survey of existing research, our work distribution mainly involved splitting off a fair amount of papers for each member to examine, as well as ensuring an equal amount of time spent on documentation. All members shared responsibility in conducting analysis of research papers. Zachary Russell was responsible for the abstract, introduction with problem statement, and approach. Brian Lasher was responsible for the evaluation and appendix results compilation. John Mulloor was responsible for the discussion and conclusion. All members were flexible and contributed to various sections as the project progressed.

7 CONCLUSION

The growth of AR, VR, and MR has demonstrated a need for computer-simulated reality devices to be properly secured. This paper evaluates biometric authentication as a mechanism for user authentication through the use of five different authentication schemes: bone conduction, optics, kinesthetics, voice, and touch. Accuracy rate, false rejection rate, false acceptance rate, and user accessibility were just some of the metrics used for the evaluation of the various mechanisms. Discussion involving future research provided a promising future for biometric authentication in computer-simulated reality devices, and cautions on the sensitivity of biometric information provided insight that needs to be taken into consideration when implementing these authentication mechanisms. Proper data handling and user due diligence are of utmost importance, or else severe consequences will arise.

We conclude by stating that biometric authentication can be safely used as a means to secure user AR/VR/MR headsets if:

- Mitigation tactics (filters, padding, noise) are applied
- Companies exercise best practices for biometric data storage, and provide support for security bugs and leaks
- Users are careful with their sensitive information

The future of this space shows promise for growth and improvement, and further research should be analyzed as new technology and ideas emerge.

REFERENCES

[1] Cong Shi, Xiangyu Xu, Tianfang Zhang, Payton Walker, Yi Wu, Jian Liu, Nitesh Saxena, Yingying Chen, and Jiadi Yu, 2021.Patricia S. Abril and Robert Plant, 2007. . Face-Mic: inferring live speech and speaker identity via subtle facial dynamics captured by AR/VR motion sensors. *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking. Association for Computing Machinery.* New York, NY, USA, 478–490. DOI: https://doi.org/10.1145/3447993.3483272

[2] Olade I, Fleming C, Liang HN. 2010. BioMove: Biometric User Identification from Human Kinesiological Movements for Virtual Reality Systems. DOI:10.3390/s20102944

[3] Brendan John, Sanjeev Koppal, and Eakta Jain, 2019. EyeVEIL: degrading iris authentication in eye tracking headsets. *In Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications (ETRA '19). Association*

for Computing Machinery. New York, NY, USA, Article 37, 1–5. DOI:https://doi.org/10.1145/3314111.3319816

[4] Mohammed Abuhamad, Ahmed Abusnaina, DaeHun Nyang, David Mohaisen, 2020. Sensor-based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey.

[5] Arman Bhalla, Ivo Sluganovic, Klaudia Krawiecka, Ivan Martinovic, 2021. MoveAR: Continuous Biometric Authentication for Augmented Reality Headsets.*CPSS '21 - Virtual Event,* June 7, 2021, Hong Kong. DOI:https://dl.acm.org/doi/pdf/10.1145/3457339.3457983

[6] Park, S.-H.; Lee, D.-G.; Park, J.-S.; Kim, J.-W. A Survey of Research on Data Analytics-Based Legal Tech. Sustainability 2021, 13, 8085. https://doi.org/10.3390/su13148085

[7] Grand View Research, 2022. Virtual Reality (VR) Market: Market-Analysis, 2018-2030.https://www.grandviewresearch.com/industry-analysis/virtual-reality-vr-market

[8] Pınar Kurtunluoglui, Beste Akdik, Tianfang Zhang, Enis Karaarslan, 2022.Security of Virtual Reality Authentication Methods in Metaverse: An Overview

[9] Z. Yu, H. -N. Liang, C. Fleming and K. L. Man, "An exploration of usable authentication mechanisms for virtual reality systems," *2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, 2016, pp. 458-460, doi: 10.1109/APCCAS.2016.7804002.

[10] Jessica Sehrt, Feng Yi Lu, Leonard Husske, Anton Roesler, Valentin Schwind, "WristConduct: Biometric User Authentication Using Bone Conduction at the Wrist" *MuC '22, September 4–7, 2022, Darmstadt, Germany*

[11] Stefan Schneegass, Youssef Oualil, Andreas Bulling, "SkullConduct: Biometric User Identification on Eyewear Computers Using Bone Conduction Through the Skull"

[12] Jarina B. Mazumdar, S. R. Nirmala, 2018. Retina Based Biometric Authentication System: A Review. International Journal of Advanced Research in Computer Science, 711-718. DOI: http://dx.doi.org/10.26483/ijarcs.v9i1.5322

[13] Shejin Thavalengal, 2015. Iris Authentication in Handheld Devices – Considerations for Constraint-Free Acquisition. IEEE Transactions on Consumer Electronics, Vol. 61, No. 2. 245-253.

[14] Peter Riendeau, 2017. Next Generation Sensors and a Potential New Ecosystem for Marketing and Advertising in Augmented and Virtual Reality. A Digital and Social Media Capstone Project, Ch. 6.

[15] Weitao Xu, Yiran Shen, Chengwen Luo, Jianqiang Li, Wei Li, Albert Y. Zomaya, Gait-Watch: A Gait-based context-aware authentication system for smart watch via sparse coding, Ad Hoc Networks,Volume 107, 2020, 102218, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2020.102218.

[16] Ioannis Papavasileiou, Zhi Qiao, Chenyu Zhang, Wenlong Zhang, Jinbo Bi, Song Han,GaitCode: Gait-based continuous authentication using multimodal learning and wearable sensors, Smart Health, Volume 19, 2021, 100162, ISSN 2352-6483, https://doi.org/10.1016/j.smhl.2020.100162.

[17] Alfred C. Weaver, Biometric Authentication, in *Computer*, vol. 39, no. 2, pp. 96-97, Feb. 2006, doi: 10.1109/MC.2006.47.

[18] Jean-François Bonastre, Frédéric Bimbot, Louis-Jean Boë, Joseph P. Campbell, Douglas A. Reynolds, Ivan Magrin-Chagnolleau, Person Authentication by Voice: A Need for Caution, In *Eighth European Conference on Speech Communication and Technology*. 2003.

[19] Taylor, Josh. "Major Breach Found in Biometrics System Used by Banks, UK Police and Defence Firms." The Guardian, Guardian News and Media, 14 Aug. 2019, https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms.

[20] Xinchen Zhang, Yafeng Yin, Lei Xie, Hao Zhang, Zefan Ge, and Sanglu Lu. 2020. TouchID: User Authentication on Mobile Devices via Inertial-Touch Gesture Analysis. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 4, 4, Article 162 (December 2020), 29 pages. https://doi.org/10.1145/3432192

[21] M. Ramya, V. Krishnaveni, K.S. Sridharan. Certain investigation on iris image recognition using hybrid approach of Fourier transform and Bernstein polynomials, Pattern Recognition Letters, Volume 94, 2017, Pages 154-162, ISSN 0167-8655, https://doi.org/10.1016/j.patrec.2017.04.009.

[22] H. Farzin, H. Abrishami-Moghaddam, and M.-S. Moin, "A novel retinal identification system," EURASIP Journal on Advances in Signal Processing, vol. 2008, no. 1, pp. 1–10, 2008.

[23] Huan Feng, Kassem Fawaz, and Kang G. Shin. 2017. Continuous Authentication for Voice Assistants. *In Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking (MobiCom '17)*. Association for Computing Machinery, New York, NY, USA, 343–355. https://doi.org/10.1145/3117811.3117823

APPENDIX

Table 5.5.1 compares the discussed authentication methods referenced in the survey.

Table 5.5.1: Comparison of Discussed Authentication Methods

Reference	Authentication Mechanism	Accuracy	False Acceptance Rate (False Negatives)	False Rejection Rate (False Positives)	Risk Mitigation Technique	Notes
SkullConduct [11]	Bone Conduction	97%	6.9%	6.9%	Incorporate additional padding in headsets to prevent listening attacks Mask stored bone conduction data using a noise pattern	Needs further research into the effects of the external environment on the reading. Accuracies based off small sample sizes
WristConduct [10]		97-98%*	0.7%	0.7%		
Iris Image Recognition [21]	Optic-Based	97%	≤ 0.5%	≤ 0.6%	Utilize a filter to dampen the quality of the iris image	Eye diseases & contact lenses could create complications Reveals health information about the user
Retinal Authentication [12]		99%	0.006%	0.006%		
Bio-Move [2]	Kinesiological	98.6%	0.00032%	1.3%	N/A	Not accessible to immobile users Requires constant movement by users in order for constant authentication to take place

VAuth [23]	Voice	97%	< 5%	< 0.1%	N/A	Can be affected by the quality of the environment and any illness producing voice-altering symptoms. The use of external peripherals could affect accuracy Not accessible by the vocally impaired The study did not specify the exact false negative rate - just emphasized that it was less than 5%
Fingerprint Reading [17]	Touch	N/A	0.01%	1.4%	N/A	Proven secure and efficient by previous technological implementations
TouchID [20]		N/A	4.9%	4.9%	N/A	Fairly high false negative and positive rates, better touch-based authentication mechanisms besides this one

*WristConduct tested two different methods for identification, support vector machines and artificial neural networks, which produced two different accuracies that fall in the range described