Secure by Design Smart Authentication for Care Robots to Support the Elderly

MAWANDA, Raymond, KEISHING, Solan, WANG, Jing <http://orcid.org/0000-0002-5418-0217> and MARCHANG, Jims <http://orcid.org/0000-0002-3700-6671>

Secure by Design Smart Authentication for Care Robots to Support the Elderly

Raymond Mawanda
Computing Department
Sheffield Hallam University
Sheffield, S1 1WB United Kingdom
raymond.mawanda@shu.ac.uk

Solan Keishing
Computing Department
Sheffield Hallam University
Sheffield, S1 1WB United Kingdom
solan.keishing@shu.ac.uk

Jing Wang
Computing Department
Sheffield Hallam University
Sheffield, S1 1WB United Kingdom
jing.wang@shu.ac.uk

Jims Marchang
Computing Department
Sheffield Hallam University
Sheffield, S1 1WB United Kingdom
jims.marchang@shu.ac.uk

Abstract—*Digital technology and innovation have transformed healthcare systems in multiple dimensions. In the dawn of this era, AI is revolutionizing the tackling of healthcare challenges by detecting and predicting medical diagnoses. On one hand, care and assistive robots are getting ready to fill the shortages of medical staff and carers in developed nations. The need for such care support is more relevant in Western society, as the older generation prefers to live independently. Such a system can provide quality independent living. However, this system deals with sensitive data of the users, so it is critical to ensure that the engagement, interaction, and access of user data are securely controlled and the privacy of the users is protected. The first line of defense in protecting the user's sensitive information is to securely identify and authenticate the user so that access is monitored and controlled. In this paper, a seamless multifactor secure-by-design authentication system using face recognition and a smartwatch is developed so that a continuous form of authentication is maintained when the user is around the robot. This ensures the robotic system is not open for its services unless the authorized user is present.*

***Keywords*— care robots, security, privacy, authentication access control, and smart devices.**

I. Introduction

[1]Robotic and AI applications have revolutionized the healthcare system. Recent research has shown the potential benefits of using intelligent robots in health and well-being, such as supporting independent living [1] and supporting individuals with autism and intellectual disability [2]. However, the healthcare sector poses unique challenges for translational research compared to other domains because the systems and devices manage sensitive and private data that must be safeguarded from being inadvertently disclosed by the robotic care AI system. In the absence of safety and security measures, the system could be attacked, manipulated, data tampered with, data leaked, data confidentiality, integrity, service availability not guaranteed, privacy compromised, and access not controlled, leading to unrestricted data and service access, system malfunctioning, misused, misdirected, misguided. It may even lead to system control by a man-in-the-middle or any cyber threat actors [3-4]. Furthermore, loss of service and system functionality, storage and memory corruption, and unreliable sensory data over an un-trustable network would be disastrous. The leaking and compromising of sensitive and private information of the user would negatively impact the user's trust, confidence, and acceptance of the system. This shows the importance of safeguarding and protecting the robot's services, sensors, and data to make the system resilient to cyber-attacks. However, security and privacy research in a care robot that is multimodal during engagement and interaction is mostly unexplored and requires further investigation to identify suitable security and privacy-preserving mechanisms and define protocols for safe engagement and interaction. In addition, the cyber-attack model in a multimodal robotic system poses a unique challenge since the vulnerabilities and attack points are many because the system is equipped with the ability to sense, process, and record the world around it through various input and output sensors. Protecting such systems from cyber-attacks is vital, particularly when these domestic robots can access individual private homes [5]. The authors of [6] explain and confirm that the difference with robotics is the ability to move and use multiple ways for recording and communicating information. This makes it more complex and more challenging to safeguard all the entry and exit points of the communication ports.

It is reported in the IBM Security X-force threat intelligence index [7] that the healthcare sector is the 7th most cyber-attacked industry in 2022. In another research report produced by IBM Security, Cybersecurity Intelligence group, it is found that over 95% of cyber security incidents are due to "human error" [8]. The most common errors include system misconfiguration, poor patch updates, use of default or easy access credentials, disclosure of information, and so on. The chances of such errors will only increase when these systems are utilised by older people who have medical and physical or psychological conditions. So, it is crucial to offload the burden of managing and controlling security techniques and mechanisms from the user without compromising the security and privacy level of the system. Thus, secure-by-design and privacy-by-design (i.e., security mechanisms should not be an

[1] For the purpose of open access, the author has applied a Creative Commons Attribution (CC BY) licence to any Author Accepted Manuscript version of this paper arising from this submission.

added application after system development but be a part of the system's design and development) are the only ways to ensure the safety and security of the robot, elderly user, and its data. Moreover, the system must be able to withstand ransomware attacks, DoS and DDoS attacks, data theft, credential harvesting, misconfiguration, malicious insider activities, etc. It is important to note that "Older people become victims of fraud every 40 seconds", as reported in research findings of AgeUK [9]. So, securing and preserving users' privacy using innovative, smart, intelligent methods that are easy to adopt and understand is vital to ensure that the user's faults and errors are limited. Thus, this paper aims to introduce a smart and secure authentication using secure-by-design interaction with multiple smart sensors (smart camera and smartwatch) to offload the pressure of authentication using multiple factors.

Mobile and Software applications used by robots use communication channels, i.e., Wi-Fi and Bluetooth, without implementing security methods [10]. The robots in the market send data either in clear text without protection or by using weak encryption. Some robots operate with weak default configurations with no permission control to allow only authorized people to access them. Due to limited secure open-source resources for developing robotic applications, most robotic programs use vulnerable open-source frameworks, e.g., Robot Operating System (ROS) with cleartext communication, weak authorization, and authentication mechanisms. Disregarding user privacy, many mobile applications of some robots send users' personal information to remote servers without their consent, as explored in [10].

II. Literature Study

A critical literature study is conducted to understand the known popular authentication techniques and their appropriateness, which may be adoptable for care robotic system users, e.g., elderly, disabled people, children in need, people with Dementia etc. The care robot deals with the sensitive and private information of the patients, so controlling who can access what information is critical, and giving the right to access is the first step to what the stakeholders can access and at what level. Since the system is used by the elderly and those in need due to their mental and physical condition, it is critical to incorporate an authentication mechanism that is easy to adopt and does not become a barrier and a burden to the user. The approach of using the traditional one-factor authentication approach is easy and simple, however, it is less secure than that of a multifactor authentication technique. The level of security can be different for single-factor or multi-factor authentication techniques. Generally, more secure mechanisms are more complex in nature, e.g., using a multi-factor technique is more secure than a single-factor mechanism, but it's more challenging to use. More complex mechanisms are not convenient to adopt either, but they safeguard the system better. So, the solution should be convenient to adopt, but at the same time, the level of security should not be compromised. Table 1 highlights and compares some of the techniques used for authentication apart from the usual PIN, password, passcode, or pattern used to identify and authenticate the authorized user.

It may be easier to remember a picture-based password [11] or a sequence of past faces or pictures to authenticate as described in [12] compared to remembering a complex alphanumeric code for the elderly. However, as the user gets older, it will become more challenging because it involves remembering. Some device-based authentication approaches, depending on the technique, may not be appropriate for an elderly user, e.g., use of the CAPTCHA method as described in [13], or use of a complex password, use of authenticator, SMS-based, or any complex knowledge-based authentication approaches will be a challenge to the elderly due to their mental state if not physical. A technique that involves OTP approaches like in [14-15] is not recommendable for the elderly because it involves additional technological knowledge and confidence to use. In fact, using personal devices like smartphones, smartwatches, etc., for authentication can be handy [16]; however, the challenge is to know if the user is using the device or if someone else is impersonating the user. When it comes to biometric authentication, it is handy because it is something the user need not carry or remember. Some of the biometric-based authentications include face recognition [17], voice [18], fingerprint-based authentication [19], and gait-based authentication [20]. However, when it involves speaking for voice identification or scanning fingerprints, it might be more challenging for the elderly than facial-based biometric authentication because it involves proactive action. The best approach is to use multifactor methods to authenticate the user, e.g., a two-factor authentication like the one mentioned in [21].

Table 1: Appropriateness and security level of authentication

Ref.	Method	Appropriate for elderly			Security Level
		No	Low	High	
[100]	Picture Passwords		✓		Low
[101]	Using Passtones		✓		Low
[102]	Invisible CAPTCHA	✓			Low
[103]	One-time password based on hash-chain	✓			Moderate
[104]	Based on OTP and hash-chains	✓			Moderate
[105]	Using personal device			✓	Moderate
[106]	Deep face recognition			✓	Moderate
[107]	Voice Biometric		✓		Moderate
[108]	Fingerprint based		✓		Moderate
[109]	Gait Based			✓	High
[110]	Two-factor with cloud		✓		High

III. The Proposed Secure by Design Authentication

This paper proposes a secure integration of multiple authentication platforms to minimize user involvement in the authentication process. The authentication involves two main components: (1) a smart camera that detects human faces and recognizes authorized users and (2) a smartwatch that detects the care robot within the radio range of the Wi-Fi signal. The smart camera that detects and recognizes users is installed at the door, hallway, and the robot, while the smartwatch is on the user's wrist. The identity information of the authorized camera and the authorized user's smartwatch are pre-registered with the robot. The face detection and recognition system runs on a robot's camera, and the smart camera is installed in the hallway and the front door. The step of the detection and recognition process is shown in Figure 1, and an example of user detection and recognition is shown in Figure 2, while Figure 3 depicts the situation when a detected face is not recognized and shows how multiple faces can also be analyzed simultaneously by the system.

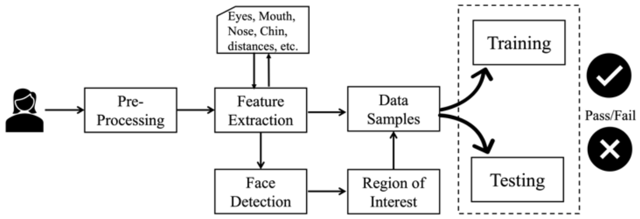
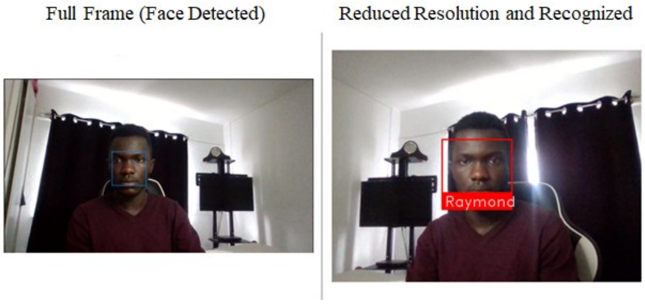


Figure 1: Face Detection and Recognition


Full Frame (Face Detected)

Reduced Resolution and Recognized

Figure 2: Example of Face Detection and Recognition

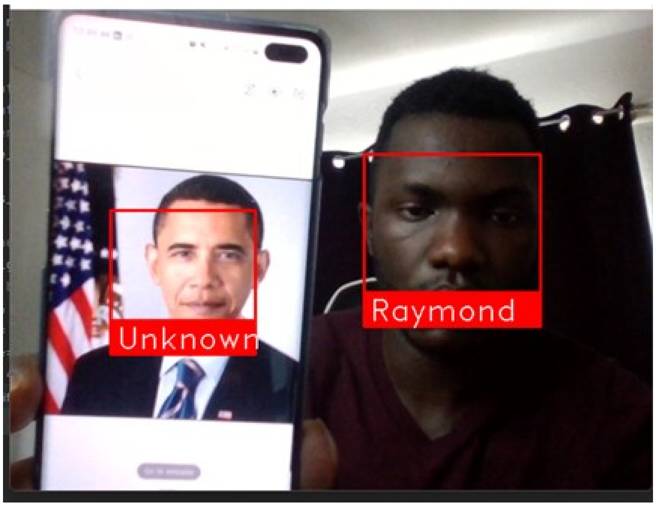


Figure 3: Recognized face and Unknown

In this study, the size of the frame is reduced to 1/4th of the original frame during the recognition process to accelerate the process. The camera is enhanced by utilizing the proximity sensor to initiate and activate the camera for face detection. This is achieved using the Dlib library (www.dlib.net), which is built using an Artificial Neural Network (ANN) model and the Histogram of Oriented Gradients (HOG) image shape feature. This model was chosen due to its high accuracy rate of 99.39%, which was pre-trained and tested using data from https://vis-www.cs.umass.edu/lfw/. A transfer learning method is applied during the training to improve the system's performance. The system was trained with 100 different image samples, containing 10 images of each person from 10 different individuals. To evaluate the performance, the system is deployed with a live video stream feed through the smart cameras to capture new face images from the same individuals for the training process. This method allows us to gather new and real-time data and assess the accuracy and effectiveness of our testing process. This approach ensures a comprehensive analysis of the proposed system's capability to recognise and identify faces accurately and efficiently.

A. Authentication Phase-1 using smart camera face detection and recognition

Figure 4 demonstrates the layout of the smart camera installation at the door or in the hallway of the house. It involves the following steps to securely detect and then engage with the robot to authenticate the user in the first step of the authentication process. Using the proximity sensor, the approaching user is detected. Then the smart camera is activated to record the detected face and proceed with the facial recognition process of the user. If the user's identity is not recorded in the whitelist of the authenticated user list, then the second authentication process (i.e., the user authentication using a smartwatch) is not necessary. However, if the face recognition is passed, the following action is invoked to securely interact with the robot from the smart camera that detected and recognized the authorized user to ensure that the process is securely captured by an authenticated and trusted camera of the user's home.

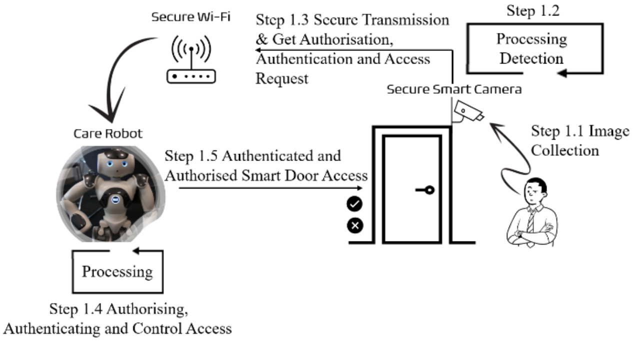

Secure Wi-Fi
Step 1.3 Secure Transmission & Get Authorisation, Authentication and Access Request
Step 1.2
Processing Detection
Secure Smart Camera
Care Robot
Step 1.5 Authenticated and Authorised Smart Door Access
Step 1.1 Image Collection
Processing
Step 1.4 Authorising, Authenticating and Control Access

Figure 4: Door or Hallway Camera Detecting and Recognizing the Authorized User.

The robot's camera is equally equipped with the face detection and recognition system, as shown in Figure 4. Following the detection of an authorized user by the smart cameras via Wi-Fi, the identity of the smart camera along with the session key, its digital signature and the detected user ID are sent to the robot securely to maintain data confidentiality and data integrity. Step 1.5 of Figure 4 to control access to the door is not tested in this paper, but it's feasible. To authenticate the smart camera and securely transfer the authorized user ID and other security parameters, the collected information (camera ID information, hash of the user ID, genesis information, session key) is securely encrypted by robot's RSA public key using equation (1) at the smart camera and decrypt using equation (2) by the robot using its private key. The key sizes used are 2048-bit and 256-bit for RSA and AES, respectively. The AES session key is updated during each interaction and engagement with the robot, and a similar approach is used when engaging between the smartwatch and the robot.

Where, $\zeta_n^{\underset{\rightarrow}{\emptyset\Delta}}$ is the genesis information of the robot ($\emptyset$) when interacting with the nth camera (Δ), that has the information consisting of a Random nonce (R_{nonce}) and Origin timestamped (O_{info}) for each robot-camera interacting pair to remember and maintain a trustable association. Where $\zeta_n^{\underset{\rightarrow}{\emptyset\Delta}}$= H ($R_{nonce}, O_{info}$) is the hashed information using SHA-256, and then it is shared by the robot to the camera securely using camera's (Δ) public key, which will be later used in authenticating the camera. The camera sent $\text{ß}_n^{\underset{\rightarrow}{\Delta\emptyset}}$ = H($\zeta_n^{\underset{\rightarrow}{\emptyset\Delta}}$+ Δ_{id}^n+ $\text{Ɣ}_{session}^{\Delta}$+ $\hat{\text{Ʊ}}_{Id}^{\Delta}$), where, $\text{Ɣ}_{session}^{\Delta}$= H$\{AES(S_{k_\Delta})\}$, user ID hashed ($\hat{\text{Ʊ}}_{Id}^{\Delta}$) = $H(User_{Id})$, the nth camera (Δ) hashed ID is given by $\Delta_{id}^n = H(\partial + MAC_\Delta)$, where a dynamic ∂ is a 64-bit Hex random value generated to uniquely identify the camera or any other device like smartwatch which is integrated with the robot and it is pre-shared during the device identity registration with the robot. This additional parameter is developed to increase the level of security during the identification and authentication process of the smart camera or smartwatch.

Table 2: Symbols of the Encryption and Decryption Processes.

Process	Symbols
Encryption using the Private key (ρ) of the camera (Δ)	E_ρ^Δ
Decryption using the public key (ξ) of the camera (Δ)	D_ξ^Δ
Encrypting using the Public Key (ξ) of the Robot ($\emptyset$)	$E_\xi^\emptyset$
Decryption using the Private key (ρ) of the Robot ($\emptyset$)	$D_\rho^\emptyset$
Encryption using the private key (ρ) of the smartwatch (ψ)	E_ρ^ψ
Decryption using the public key (ξ) of the smartwatch (ψ)	D_ξ^ψ
Session key of the camera (Δ)	$AES(S_{k\_\Delta})$
Session key of smartwatch (ψ)	$AES(S_{k\_\psi})$
Serial number or Electronic Serial Number	ESN_{Id}
International Mobile Equipment Identity	$IMEI_{Id}$
ID of a user (hash of the ID)	$User_{Id}$
MAC address of the smart camera	MAC_Δ
MAC address of smartwatch	MAC_ψ
A 64-bit Hex random value for a smart camera	∂

$$\omega_\Delta = E_\xi^\emptyset\left[\Delta_{id}^n, User_{Id}, AES(S_{k\_\Delta}), E_\rho^\Delta\left\{\text{ß}_n^{\underset{\rightarrow}{\Delta\emptyset}}\right\}\right] \tag{1}$$

$$\text{Ʊ}_\emptyset = D_\rho^\emptyset(\omega_\Delta) \tag{2}$$

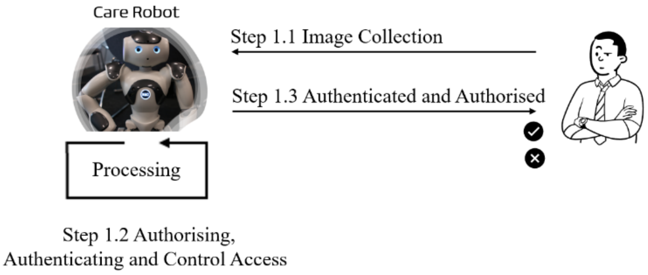

Care Robot
Step 1.1 Image Collection
Step 1.3 Authenticated and Authorised
Processing
Step 1.2 Authorising,
Authenticating and Control Access

Figure 5: Robot Camera Detecting and Recognizing the Authorized User.

When the user is in sight of the robot, face detection and recognition is initiated by the robot's smart camera. In such a case, camera authentication and invoking the secure interaction is not considered. However, in an actual Robotic Operating System (ROS), since it works under a publish and subscribe model where a node can send information to a topic and other nodes can subscribe, a secure module is required during the interaction and engagement within various nodes and modules. However, that aspect is not considered in this paper since the camera module of the robot is interacting within the robot and not publishing for any external nodes.

B. Authentication Phase-2 using Smartwatch

In the second phase of authentication, smartwatches are considered to ensure mobility and continuity of the authentication if the user is within the robotic network range. This can be done in two ways: via a Wi-Fi network or Bluetooth. In this paper, the connection is done via a Wi-Fi router where the camera and the robot are connected. The Wi-Fi router can be a part of the robotic system; however, in this study, the Wi-Fi router is external to the robot, and the robot acts as a node of this home Wi-Fi network. Figure 4 shows the interaction and engagement between the user's smartwatch and the robot. The smartwatch encrypts the information using the public key of the robot, as shown in equation (3), and the robot decrypts using equation (4). However, information will not be sent to the robot until the user initiates the process by entering the PIN of the smartwatch, which is a way to know that the authorized user triggers the authentication process. The steps are displayed in Figure 7. Moreover, this triggering process is considered valid only when the watch is attached to the user's wrist (using an off-body sensor of the smartwatch). The authentication of the user is considered valid only after the two phases of the authentication process are completed. This smartwatch has the following configuration: 1.5GB RAM + 16GB Internal Memory, LTE, Bluetooth® 5.0, Wi-Fi 802.11 a/b/g/n 2.4+5GHz, wear OS 4.0, Android System 13. The smart devices connect with the robot over a 2.4GHz Wi-Fi network.

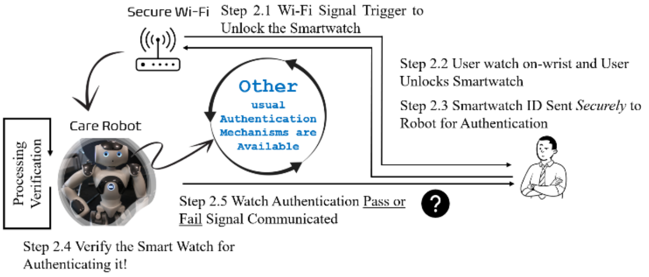

Secure Wi-Fi
Step 2.1 Wi-Fi Signal Trigger to Unlock the Smartwatch
Step 2.2 User watch on-wrist and User Unlocks Smartwatch
Step 2.3 Smartwatch ID Sent Securely to Robot for Authentication
Other usual Authentication Mechanisms are Available
Care Robot
Processing Verification
Step 2.5 Watch Authentication Pass or Fail Signal Communicated
?
Step 2.4 Verify the Smart Watch for Authenticating it!

Figure 6: Smartwatch of Authorized User Detection and Authentication.

Smartwatch Identity and encrypt using Robot's public key:

$$\omega_\psi = E_\xi^\emptyset\left[\Delta_{id}^m, \psi_{id}^n, AES(S_{k\_\psi}), E_\rho^\psi\left\{\text{ß}_m^{\underset{\rightarrow}{\psi\emptyset}}\right\}\right] \tag{3}$$

$$\text{Ʊ}_\emptyset = D_\rho^\emptyset(\omega_\psi) \tag{4}$$

Where, $\zeta_m^{\underset{\rightarrow}{\emptyset\psi}}$ is the genesis information of the robot ($\emptyset$) when interacting with the mth smartwatch (ψ), that has the information consisting of Random nonce (R_{nonce}) and Origin timestamped (O_{info}) for each robot-smartwatch interacting pair. Where $\zeta_m^{\underset{\to}{\emptyset\psi}}$= H($R_{nonce}, O_{info}$) is the hashed information using SHA-256, it is shared by the robot to the smartwatch securely using smartwatch's (ψ) public key, which will be later used in authenticating the smartwatch. The smartwatch sent $ß_m^{\underset{\to}{\psi\emptyset}}$ = H($\zeta_m^{\underset{\to}{\emptyset\psi}}$+ Δ_{id}^m+ $Ɣ_{session}^{\psi}$), where , $Ɣ_{session}^{\psi}$= H$\{AES(S_{k_\psi})\}$, the mth smartwatch (ψ) ID is given by $\Delta_{id}^m = ESN_{Id} + IMEI_{Id} + MAC_{\psi} + \partial$.

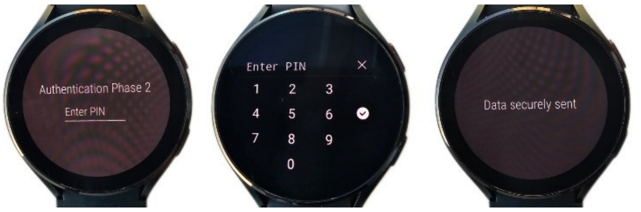


Figure 7: Smartwatch Authentication Initiation from the user

C. Integration of the multifactor features

Facial recognition is the first step of the authentication process, and the second phase includes authenticating the user's watch, as described in section B. However, to guarantee that watch data is generated from the authorized watch, two additional factors are considered, i.e., (i) the authorized user must open the watch authentication initiation app on the smartwatch and enter their passcode to activate the watch authentication process and (ii) this app functions as a positive command only if the watch is on the user's wrist. The algorithm of the multifactor authentication integration is listed in Table 3 where f = face image, Δ = camera, ψ = smartwatch, $\mathscr{H}$ = On_wrist, Ꝑ = passcode (), $User_{Id}$ = Identified user, T = True.

Table 3: Multifactor Authentication Integrator

```
Procedure ($f$, $\Delta$, $\psi$ , $\mathscr{H}$, Ꝑ)
index $\longleftarrow$ 0, no_cam $\longleftarrow$ 0, sw $\longleftarrow$ 0
$\mathscr{H} \longleftarrow$ F , Ꝑ $\longleftarrow$ F
$User_{Id} \longleftarrow$ face_detection(f)
repeat
  $User_{Id} \longleftarrow$ face_detection(f)
  if ($User_{Id}$= Authenticated_User) then
    repeat
      $\Delta \longleftarrow$ Camera_f (camera_ID)
      if ( $\Delta$ = Authenticated_Camera) then
        repeat
          $\psi \longleftarrow$ Smartwatch_f(watch_ID)
          if ($\psi$ = Auth_Smartwatch && $\mathscr{H}$==T && Ꝑ==T) then
            Access $\longleftarrow$ Data
          else continue
        until sw < p
      else continue
    until no_cam < m
  else continue
until index < n
```

IV. Results and Discussion

This section covers the analysis of the mechanisms and techniques used in detecting, recognizing, and authenticating the devices and the user to follow a secure-by-design authentication mechanism.

A. Face detection and recognition

The facial detection and recognition system is based on the HOG feature. After normalizing the feature space before training, the HOG component becomes scale-invariant, so the size of the picture does not significantly affect the study. During the study, the original video/image size captured was reduced to 1/4th to improve processing time. When a video is captured, the face in every frame is detected and recognized, but it does not impact the accuracy of the detection rate. However, it reduces processing time during feature extraction. For example, when the reduced frame is 500 x 666 pixels compared to 400 x 400 pixels, the training period for detecting and recognizing a face is only 7.50% longer for the lesser resolution frame.

The AI for facial detection and recognition is so effective that it can detect the user uniquely from a printed picture, digital picture, video, etc., which is a drawback. Learning that the captured image or video comes from a real human user standing before the camera is vital. It is possible and is achieved using a depth camera, e.g., the "TrueDepth" camera used by the latest iPhone, by truly mapping the geometry of the user's face for facial ID recognition or using multiple cameras to create a depth effect. In such a design and development, the cost is higher, and overheads are always an issue. In this paper, a very simple HD camera is used, equipped with a lightweight computational system (Raspberry Pi) with a 1.5 GHz 64-bit quad-core ARM Cortex-A72 processor onboard 802.11ac Wi-Fi.

B. Security analysis on smart device interaction

Data confidentiality and integrity of the interaction and engagement between the smart devices (camera and smartwatch) and the robot is well preserved using two-fold encryption techniques, i.e., RSA and AES cryptography. The use of asymmetric key cryptography allows digital signing of the data, enables certificate-based authentication of the source, and the secure exchange of the session key without the need for any additional key exchange mechanism. Encrypting $\zeta_n^{\underset{\to}{\emptyset\Delta}}$ and $\zeta_m^{\underset{\to}{\emptyset\psi}}$ using the smart device's respective public keys ensures that the genesis information sent by the robot is made visible only to the associated peers and signing it using the robot's private key guarantees the origin of the source. Encrypting the $E_\rho^{\Delta}\left\{ß_n^{\underset{\to}{\Delta\emptyset}}\right\}$ and $E_\rho^{\psi}\left\{ß_m^{\underset{\to}{\psi\emptyset}}\right\}$ using the private key of the respective camera and the smartwatch ensures that non-repudiation attack is impossible. Thus, the transiting data between the robot and the smart devices is non-forgeable, non-reuseable, and non-alterable by any third party or a man-in-the-middle. Each device's identity is a hash of multiple values it is associated with, including the MAC address and pseudo-random (∂) 64-bit Hex value. The hashing of multiple identity information, i.e., $ESN_{Id}, IMEI_{Id}, MAC_{\psi}$ and ∂ for the smartwatch is to make a spoofing attack impossible even if the man-in-the-middle spoofed the device's IP and MAC addresses, making it more resilient. The system availability is restricted based on the signal of the home Wi-Fi network and the association of the pre-registered smart devices. However, remote access and authentication of the authorized user can also be conducted if the user's facial recognition can be associated with their presence and their smartwatch all at the same time and in the same place. Once the face detection and recognition are successful, the care robot waits for the follow-up features to complete the authentication process, i.e., securely identify and recognize the smartwatch of the user by prompting the user to unlock the phone, leading to securely transmitting the watch identity when it is on the user's wrist making it secure by design during an interaction and engagement with the care robot.

C. *Security Overhead and Performance Analysis*

The system runs 100 times using RSA 2048-bit key for public-private key, AES 256-bit session key, and SHA 256-bit key for signing, and an average is calculated for the overheads incurred by the security mechanisms and the delay it causes in the interaction and engagement with the robotic system. In the smartwatch, the average time for securing the identity information, genesis data, session key, and digital signature information takes 0.12ms; however, the process of creating the digital signature takes 14.88ms. While on the care robot, it took 1.05ms on average to decrypt the received data and 0.87ms to verify the digital signature it received. However, the average time for delivering the data from the smartwatch to the robot is 0.31ms, which involves the time of flight and the queuing delay.

V. Conclusion and Future Direction

Authentication is the first line of defense in controlling access to any system and its services. So, incorporating mechanisms to authenticate any device and user is vital in keeping the system and its data safe. Single-factor authentication is easy to use but is less secure than the multifactor framework. However, multifactor authentication mechanisms can be daunting to use with ease, especially for the elderly due to age-related issues. So, this paper proposes a smart multifactor authentication system that doesn't involve remembering additional information to authenticate the user securely, using a secure facial recognition system integrated with the user's smartwatch. In this research, the system not only relies on the multifactor for the authentication process but also authenticates the devices capturing the identities of the users to maintain a high level of trust with the data-generating sources, making the mechanism secure by design. The first factor uses a securely connected smart camera of the robot or any securely connected smart camera of the house to conduct face recognition of the user. The second factor uses three additional features for authentication, i.e., the user's smartwatch, its pin to initiate the authentication of the smartwatch and finally, the watch must be on the user's wrist to complete the authentication process. This mechanism does not involve remembering complex passwords or a separate PIN but the code for locking and unlocking the smartwatch, which is likely to be remembered by the user. Because usability is one of the key issues among the elderly, the paper aims to make the authentication process easy to adopt while the complexity of the entire process is hidden from the user. Otherwise, the authentication mechanism will become a barrier and a burden to the robot user.

The future work includes an extensive study of the usability of the system among potential elderly users. A test about the ease of use of the mechanisms among the potential users is also required. It requires quantitative and qualitative studies to understand more about the mechanism's acceptability, accuracy, and convenience among potential users.

References

[1]. Di Nuovo, A., Broz, F., Wang, N., Belpaeme, T., Cangelosi, A., Jones, R., & Dario, P. (2018). The multi-modal interface of Robot-Era multi-robot services tailored for the elderly. INTELLIGENT SERVICE ROBOTICS (1861-2776), 11(1), 109-126.

[2]. Di Nuovo, A.; Conti, D.; Trubia, G.; Buono, S.; Di Nuovo, S. (2018). Deep Learning Systems for Estimating Visual Attention in Robot-Assisted Therapy of Children with Autism and Intellectual Disability. ROBOTICS (2218-6581), 7(2): 25.

[3] Marchang, J., Di Nuovo, A., Elliott, C., Meese, H., Vinanzi, S. and Zecca, M., 2023. Security and privacy in assistive robotics: cybersecurity challenges for healthcare. White paper, report, EPSRC, UK-RAS Network.

[4]. Marchang, J. and Di Nuovo, A., 2022. Assistive multimodal robotic system (AMRSys): security and privacy issues, challenges, and possible solutions. *Applied Sciences*, *12*(4), p.2174.

[5]. Urquhart, L., Reedman-Flint, D., & Leesakul, N. (2019). Responsible domestic robotics: exploring ethical implications of robots in the home. Journal of Information, Communication and Ethics in Society.

[6]. Calo, M. R. (2020). Chapter 12 Robots and Privacy. In Machine Ethics and Robot Ethics (pp. 491-505). Routledge.

[7] IBM security, X-force Threat Intelligence Index, 2023 Report. https://www.ibm.com/downloads/cas/DB4GL8YM

[8]. IBM Security Services Cyber Security Intelligence Index (2014), IBM Global Technology Services Managed Security Services, Research Report.

[9].https://www.ageuk.org.uk/latest-press/articles/2019/july/older-person-becomes-fraud-victim-every-40-seconds/ (Published on 31 July 2019, accessed on 13/11/2023).

[10] Cerrudo, C. and Apa, L., 2017. Hacking robots before Skynet. *IOActive Website*, pp.1-17.

[11] Hadjidemetriou, G., Belk, M., Fidas, C. and Pitsillides, A., 2019, May. Picture passwords in mixed reality: Implementation and evaluation. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-6).

[12] Brown, M. and Doswell, F.R., 2010, April. Using passtones instead of passwords. In *Proceedings of the 48th Annual Southeast Regional Conference* (pp. 1-5).

[13] Guerar, M., Merlo, A., Migliardi, M. and Palmieri, F., 2018. Invisible CAPTCHA: A usable mechanism to distinguish between malware and humans on the mobile IoT. *computers & security*, *78*, pp.255-266.

[14] Park, C.S., 2018. One-time password based on hash chain without shared secret and re-registration. *Computers & Security*, *75*, pp.138-146.

[15] Chenchev, I., Nakov, O. and Lazarova, M., 2021. Security and performance considerations of improved password authentication algorithm, based on OTP and hash-chains. In *Proceedings of the Future Technologies Conference (FTC) 2020, Volume 3* (pp. 921-934). Springer International Publishing.

[16] Alhothaily, A., Hu, C., Alrawais, A., Song, T., Cheng, X. and Chen, D., 2017. A secure and practical authentication scheme using personal devices. *IEEE access*, *5*, pp.11677-11687.

[17] Zulfiqar, M., Syed, F., Khan, M.J. and Khurshid, K., 2019, July. Deep face recognition for biometric authentication. In *2019 international conference on electrical, communication, and computer engineering (ICECCE)* (pp. 1-6). IEEE.

[18] Singh, N., Agrawal, A. and Khan, R.A., 2018. Voice biometric: A technology for voice based authentication. *Advanced Science, Engineering and Medicine*, *10*(7-8), pp.754-759.

[19] Dass, S.C., 2013. Fingerprint-Based Recognition. *International Statistical Review*, *81*(2), pp.175-187.

[20] Cola, G., Avvenuti, M., Musso, F. and Vecchio, A., 2016, November. Gait-based authentication using a wrist-worn device. In *Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services* (pp. 208-217).

[21] Derhab, A., Belaoued, M., Guerroumi, M. and Khan, F.A., 2020. Two-factor mutual authentication offloading for mobile cloud computing. *IEEE Access*, *8*, pp.28956-28969.