Research Article OPEN ACCESS

Cloud-Based Gait Biometric Identification in Smart Home Ecosystem

Anusha Bodepudi
Staff Engineer, Intuit, Plano, TX, USA,
Anusha_bodepudi@intuit.com

Manjunath Reddy
Customer Engineering Lead, Qualcomm , San diego, CA, USA,
reddymanjushari@gmail.com

Abstract

As smart homes continue to proliferate, ensuring robust security measures becomes a pressing concern. Traditional authentication methods such as passwords and PINs are increasingly vulnerable to sophisticated attacks. This research proposes the implementation of cloud-based gait biometric identification in a smart home ecosystem to address these security challenges. By integrating gait recognition technology with the cloud, this study aims to enhance smart home security while providing a seamless and reliable access control mechanism. The research explores the enrollment process, gait biometric authentication, and access control within the smart home ecosystem. Additionally, it investigates the integration of real-time monitoring and security alerts, enabling prompt responses to potential threats. The cloud-based approach offers scalability, privacy, and data integrity, making it suitable for multiple residents and expanding smart home infrastructures. This research contributes to the growing body of knowledge on biometric authentication and IoT security, offering a viable solution to safeguard the smart homes of the future.

Keywords: Smart homes, Gait biometric identification, Cloud-based security, Access control, IoT security

Declarations

Competing interests:

The author declares no competing interests.

Introduction

Smart homes have emerged as a dominant trend in the modern technological

landscape, as homeowners seek to harness the power of IoT devices to enhance convenience, security, and energy efficiency within their living spaces [1], [2]. These interconnected systems enable seamless communication between diverse devices, including smart thermostats, lighting controls, smart appliances, security cameras, and voice-controlled assistants [3]. The integration of these IoT devices facilitates a holistic and intelligent living environment where occupants can easily manage and automate various aspects of their home with the touch of a button or a simple voice command [4]. By allowing different devices to collaborate and share data, smart homes empower residents to optimize their daily routines, reduce energy consumption, and enjoy enhanced comfort and safety [5].

Smart home systems consist of various components that work together to automate and enhance the functionality of a house [6]. One essential component is the smart hub or central controller. The smart hub serves as the brain of the smart home, connecting and coordinating all the devices and sensors within the system. It enables seamless communication between different devices, allowing users to control and monitor their home remotely. The smart hub often utilizes wireless protocols like Wi-Fi, Zigbee, or Z-Wave to connect with compatible devices, such as smart lights, thermostats, security cameras, and smart appliances. Another crucial component of a smart home is the intelligent sensors [7]. These sensors detect and monitor various environmental conditions within the house, providing valuable data to the smart system [8]. For instance, motion sensors can detect movement and trigger actions like turning on lights or activating security cameras. Door and window sensors can alert homeowners if they are left open or tampered with [9] [10]. Temperature and humidity sensors help regulate the indoor climate by adjusting the thermostat accordingly. These sensors contribute to energy efficiency, security, and convenience by automating tasks and providing valuable insights about the home environment [9].

Smart home components also include actuators, which are responsible for carrying out physical actions based on the instructions received from the smart hub or user commands. Actuators can include smart switches, smart locks, motorized blinds, and smart appliances [11]. For example, a smart switch can remotely control the power supply to lights or electrical outlets, allowing users to turn them on or off using a mobile app or voice commands [12]. Smart locks provide enhanced security by allowing keyless entry and remote access monitoring. Motorized blinds can be automated to adjust based on natural light or time of day. Actuators empower homeowners to control and interact with their smart home devices, adding convenience and customization to their living spaces [13].

As smart homes become more prevalent, they become an attractive target for cybercriminals and malicious actors [14]. These individuals exploit vulnerabilities in connected devices to gain unauthorized access or control over various aspects of a smart home. A breach in a smart home's security can have serious consequences. It can start with simple inconveniences such as unauthorized access to household devices, leading to disruptions in daily routines or unexpected behavior of smart appliances. For example, an intruder

gaining access to a smart door lock could enter the house undetected.

Beyond these inconveniences, the consequences can escalate to more severe threats. Home intrusion is a significant concern, as malicious actors could exploit vulnerabilities in security systems to gain unauthorized access to a property [15]. This could result in theft or damage to personal belongings, leading to financial loss and emotional distress for homeowners. Furthermore, compromising personal data is another major risk. Smart home devices often collect and store sensitive information, such as user preferences, usage patterns, and even audio or video recordings [16]. If these data fall into the wrong hands, individuals' privacy can be violated, and they may become targets of identity theft or other forms of cybercrime.

A biometric system is a technological solution that is designed to authenticate or verify the identity of individuals based on their unique physical or behavioral characteristics [17]. It utilizes advanced algorithms and specialized sensors to capture and analyze these characteristics, ensuring a highly accurate and secure method of identification. The process typically involves three main stages: enrollment, storage, and verification [18].

During the enrollment phase, an individual's biometric data is collected and stored in a database. This data can include fingerprints, facial features, iris patterns, voice samples, or even behavioral traits such as gait or keystroke dynamics. The person's biometric information is captured using specialized sensors, such as fingerprint scanners, cameras, or microphones. The data is then processed to create a digital template or reference that represents the unique features of the individual's biometric traits. This template is securely stored in a database for future comparison [19].

In the storage stage, the biometric template is securely stored in a database with appropriate encryption and access controls [20]. It is important to note that in most secure biometric systems, the actual raw data is not stored. Instead, a mathematical representation of the data, such as a set of numerical values or algorithms, is stored. This ensures that even if the database is compromised, it would be nearly impossible to reconstruct the original biometric data.

During the verification phase, when an individual seeks to access a system or authenticate their identity, their biometric traits are captured again and compared against the stored template. The system analyzes the newly captured biometric data and performs a matching algorithm that compares it to the stored template. If the system finds a close enough match, it confirms the identity of the individual, granting them access or authentication. The matching algorithm employs sophisticated techniques to handle variations in biometric traits due to factors such as changes in lighting conditions, aging, or minor injuries.

In a smart home, biometrics can be integrated into various devices and systems, such as smart locks, security cameras, and voice assistants, to provide personalized and seamless user experiences [21]. One of the primary applications of biometric systems in the smart home ecosystem is access control. Smart locks can be equipped with fingerprint scanners, facial recognition, or even iris recognition technology to allow homeowners and authorized individuals easy and secure entry into the house. This eliminates the need for traditional physical

keys, which can be lost or stolen, and reduces the risk of unauthorized access. Additionally, biometric access control systems can be integrated with user profiles, enabling the smart home to recognize different family members or frequent visitors, customizing the environment to their preferences in terms of lighting, temperature, and entertainment options [22].

Furthermore, biometric systems enhance the security of the smart home by providing multifactor authentication. In addition to traditional methods like passwords or PINs, biometric traits such as fingerprints or voiceprints can be used as an additional layer of security. For example, a smart home security system can require both a password and a fingerprint scan to disarm the alarm, ensuring that only authorized users can access the system's controls. This advanced security measure significantly reduces the risk of unauthorized access to critical smart home functionalities and personal data.

Beyond access control and security, biometrics also contribute to the seamless integration and automation within the smart home ecosystem. For instance, voice assistants equipped with voice recognition technology can accurately identify different household members and personalize responses and services accordingly. This enables a more natural and efficient interaction with the smart home, as users can issue voice commands without explicitly stating their identity. Moreover, behavioral biometrics, such as gait recognition, can be utilized to enhance the overall user experience by adapting smart home functionalities based on individual walking patterns or behavioral patterns. This could lead to automatic adjustments in lighting, climate control, and entertainment systems as a person moves around the house.

Gait Biometrics

Gait biometrics is a method of human identification and authentication that utilizes the unique characteristics of an individual's walking pattern [23]. It is based on the understanding that every person has a distinct gait, influenced by various factors such as body structure, posture, and movement patterns. Gait biometrics systems typically consist of specialized sensors, such as accelerometers or video cameras, to capture and analyze the gait data [24], [25].

The process of gait biometrics begins with data acquisition, where the sensors record the individual's walking pattern. In the case of accelerometer-based systems, the sensors are typically attached to the individual's lower limbs, such as the ankles or shoes, to capture the acceleration and orientation of the body during walking. Video-based systems, on the other hand, use multiple cameras to capture the movement of the entire body. This raw gait data is then processed and transformed into a format suitable for analysis.

Feature extraction is a crucial step in gait biometrics, where the relevant information is extracted from the raw gait data. Various techniques, such as principal component analysis (PCA) or discrete wavelet transforms (DWT), can be employed to extract meaningful features. These features may include parameters related to step length, stride duration, joint angles, or energy distribution during walking. By extracting these distinctive gait features, a unique gait signature for each individual can be created.

The final step in gait biometrics is pattern matching or classification. In this phase, the extracted gait features are compared to a pre-established database of gait signatures. This database contains the gait profiles of known individuals. The matching algorithm calculates the similarity between the extracted features and the stored gait signatures, typically using techniques like dynamic time warping or Euclidean distance metrics. Based on this comparison, the system determines the identity of the individual by selecting the closest match or applying a threshold for authentication.

Cloud-Based Gait Biometric Identification

Table 1. flow of the proposed cloud-based gait biometric identification in smart home ecosystem

Step	Detail
Step 1	**Enrollment**
	The residents enroll in the cloud gait recognition system by providing a set of gait data.
	The gait data is collected through specialized sensors or cameras installed within the home's entrance areas.
Step 2	**Gait Biometric Authentication**
	When a resident approaches the smart home's entrance, the smart camera or sensor captures the resident's gait.
	The captured gait data is encrypted and sent to the cloud gait recognition system for analysis.
	The cloud-based system compares the gait data against the enrolled patterns to verify the resident's identity.
Step 3	**Access Control and Home Functionality**
	Upon successful gait authentication, the cloud-based system sends an access signal back to the smart home ecosystem.
	The smart home ecosystem grants access to authorized functionalities such as unlocking the front door, adjusting lighting, temperature, or other personalized settings.
Step 4	**Real-time Monitoring and Security Alerts**
	The smart home security cameras continue to monitor the premises for any suspicious activities.
	In case of any unauthorized access attempts, the cloud-based system can trigger real-time security alerts to the homeowners' mobile devices.

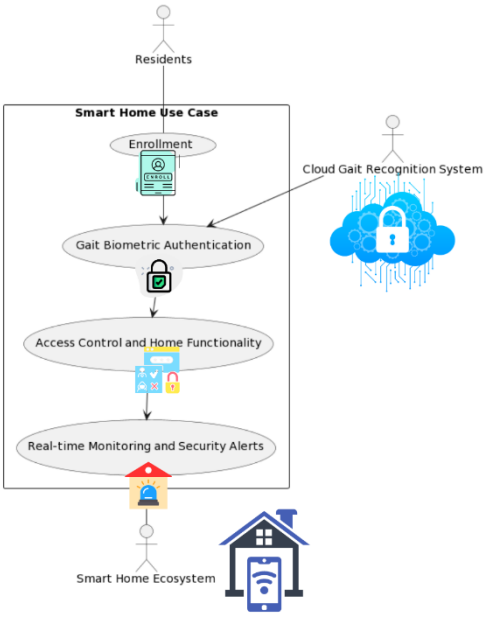
The proposed cloud gait recognition system operates through several steps to provide secure access control and home functionality. The first step is enrollment, where residents participate by providing a set of gait data. This data is collected using specialized sensors or cameras installed within the home's entrance areas. By analyzing the unique characteristics of an individual's gait, such as their stride length and walking pattern, a personalized gait profile is created for each resident.

In the second step, gait biometric authentication, when a resident approaches the smart home's entrance, a smart camera or sensor captures their gait. The captured gait data is then encrypted and transmitted to the cloud gait recognition system for analysis. Using advanced algorithms, the cloud-based system compares the received gait data against the enrolled patterns to verify the resident's identity. This process helps ensure that only authorized individuals are granted access to the smart home.

Upon successful gait authentication in step three, the cloud-based system sends an access signal back to the smart home ecosystem. This signal enables the smart home to grant access to authorized

functionalities. For example, the front door can be automatically unlocked, and personalized settings such as lighting and temperature can be adjusted according to the resident's preferences. This integration of gait recognition with the smart home ecosystem enhances convenience and security, as residents can seamlessly access and control their homes based on their unique gait patterns.

Figure 1. Cloud-based gait recognition system design



In the fourth step, real-time monitoring and security alerts come into play. The smart home security cameras continue to monitor the premises for any suspicious activities even after the initial gait authentication. In the event of any unauthorized access attempts, the cloud-based system is capable of triggering real-time security alerts. These alerts can be sent to the homeowners' mobile devices, providing them with instant notifications and updates about potential security breaches. By leveraging real-time monitoring and security alerts, the cloud gait recognition system helps ensure the safety and protection of the smart home and its residents.

At the core of this system lies the User Profile, which is characterized by a Unique User ID and the User Name. This profile is associated with Gait Biometric Data, which comprises the distinctive gait patterns of each enrolled user, enabling biometric identification.

The Cloud Gait Recognition System acts as the centralized repository for all enrolled user profiles. It houses the Gait Biometric Database, which securely stores the gait data of users for seamless authentication. Additionally, the system maintains detailed Authentication Logs, recording timestamps and success/failure status for every authentication attempt, ensuring accountability and monitoring access activity.

Within the Smart Home Ecosystem, an array of IoT Devices work in harmony to create an interconnected and intelligent living space. These devices include smart locks, cameras, lighting systems, temperature control, and more. The Device Access Control aspect of the system manages access permissions based on the user's authenticated status, guaranteeing that only authorized users can operate specific devices or functionalities.

Security is of paramount importance, and the Smart Home Security module ensures a robust defense. Security Camera Feeds provide live or recorded video feeds from cameras installed throughout the smart home, allowing homeowners to monitor their premises remotely. Furthermore, the system issues real-time Security Alerts,

immediately notifying homeowners of unauthorized access attempts or suspicious activities to facilitate prompt action.

The Integration Interfaces play a crucial role in enabling seamless communication and interaction between various components. The Gait Sensor/Camera Interface efficiently captures gait data from sensors or cameras installed at the entrance areas, facilitating biometric authentication. The Cloud API establishes a communication channel between the smart home ecosystem and the cloud-based gait recognition system, streamlining the authentication process and access control. To ensure data integrity and privacy, secure Communication Protocols are employed. These protocols implement encryption to safeguard the transmission of gait biometric data and authentication results between the smart home ecosystem and the cloud system. Additionally, Device Control Protocols govern communication between the smart home ecosystem and IoT devices, enabling effective control over granting or denying access based on user authentication status.

Gait biometric identification provides an advanced and robust authentication method that enhances the security of the smart home ecosystem. Unlike traditional methods such as passwords or keycards, gait biometrics are inherently unique to each individual and difficult to forge or replicate. The distinctive gait patterns captured by the system make it extremely challenging for unauthorized individuals to mimic or imitate, minimizing the risk of unauthorized access to the smart home.

By leveraging gait biometric data, the system ensures that only enrolled users with verified identities can gain access to the smart home and its connected devices. This eliminates the vulnerabilities associated with lost or stolen keys, as well as the potential for password breaches or unauthorized sharing. The system's reliance on an individual's unique gait patterns provides an additional layer of security that significantly reduces the chances of unauthorized entry, protecting the privacy and safety of the residents and their belongings.

One of the key benefits of utilizing gait biometric identification within the smart home ecosystem is the seamless user experience it offers to residents. With this authentication method, residents can access their smart home devices effortlessly, eliminating the need for physical keys or remembering complex passwords. The system automatically recognizes the individual based on their gait patterns, granting them seamless and convenient access to their personal devices and functionalities.

Residents no longer need to fumble for keys or worry about forgetting or misplacing them. They can simply walk up to the entrance area, and the gait sensors or cameras capture their unique gait patterns, swiftly granting access. This streamlined process saves time and eliminates the hassle associated with traditional authentication methods.

Moreover, the seamless user experience extends beyond just entering the smart home. Once inside, residents can interact with various IoT devices without the need for additional authentication steps. Lighting systems, temperature control, security cameras, and other devices can be effortlessly controlled through the smart home ecosystem, enhancing convenience and making daily tasks more efficient. The gait biometric identification technology

seamlessly integrates into the residents' lifestyle, creating a truly user-friendly and intuitive smart home experience.

Cloud-based gait recognition brings a high level of scalability to the smart home ecosystem, making it capable of accommodating multiple residents and expanding home environments. By leveraging the power of cloud computing, the system can handle a large number of user profiles and gait biometric data with ease. This scalability is crucial as smart homes continue to grow in popularity and more residents embrace the convenience and benefits they offer.

With cloud-based infrastructure, the system can efficiently store and manage the extensive data associated with gait biometric identification. The cloud allows for seamless integration of new user profiles and gait data, making it easy to enroll additional residents into the smart home system. Whether it's a single-family home or a multi-unit dwelling, the cloud-based gait recognition system can adapt and scale accordingly, providing a flexible and future-proof solution.

The scalability of the cloud-based system also extends to the smart home ecosystem itself. As residents add more IoT devices to their homes, such as additional cameras, locks, or smart appliances, the system can seamlessly integrate these new devices and expand its functionalities. This ensures that the smart home ecosystem can keep up with the evolving needs and preferences of the residents, providing a scalable and adaptable solution.

Data privacy is a critical concern in any technology that deals with personal information. Cloud-based gait recognition systems prioritize the privacy and security of gait biometric data through advanced encryption and access controls. This ensures that the sensitive data collected from residents' gait patterns remains confidential and protected.

Encryption plays a vital role in safeguarding the transmission and storage of gait biometric data. Secure encryption protocols are utilized to encrypt the data during transmission between the smart home ecosystem and the cloud-based system. Additionally, the data stored in the cloud is encrypted at rest, adding an extra layer of protection against unauthorized access.

Access controls are implemented to restrict and monitor who can access the gait biometric data. Only authorized personnel, such as system administrators or authenticated users, are granted access to the data. The cloud-based system employs robust user authentication mechanisms, such as strong passwords or multi-factor authentication, to ensure that only authorized individuals can view or manage the gait biometric data. Furthermore, stringent privacy policies and compliance measures are put in place to govern the handling of personal data. These policies align with relevant data protection regulations to ensure that residents' privacy rights are respected, and their data is handled in a responsible and lawful manner.

Conclusion

this research has proposed the implementation of cloud-based gait biometric identification as a robust security measure in smart homes. The study has demonstrated the potential of integrating gait recognition technology with the cloud to enhance smart home security while providing a seamless and reliable access control mechanism.

The research has explored various aspects of the proposed solution, including the enrollment process, gait biometric authentication, and access control within the smart home ecosystem. It has also investigated the integration of real-time monitoring and security alerts to enable prompt responses to potential threats. By utilizing the cloud-based approach, this research has highlighted the advantages of scalability, privacy, and data integrity, which are crucial for accommodating multiple residents and expanding smart home infrastructures. The cloud-based gait biometric identification system offers an efficient and effective means of securing the smart homes of the future. This research contributes to the growing body of knowledge on biometric authentication and IoT security. By presenting a viable solution to address the pressing security challenges in smart homes, this study lays the foundation for further research and development in this field.

Gait recognition technology, although promising, is susceptible to various factors that can impact its accuracy and reliability. One such factor is changes in footwear, as different types of shoes can alter a person's gait pattern. Researchers need to address this issue by conducting studies that examine the impact of footwear on gait biometric identification. By understanding how different shoes affect gait recognition, more robust and accurate algorithms can be developed to handle real-world scenarios where individuals may wear different types of footwear.

Furthermore, the health conditions of individuals can also affect their gait patterns. For instance, injuries or physical disabilities may cause variations in the way people walk. It is crucial for researchers to investigate how such health conditions can impact the performance of gait recognition systems. By accounting for these factors, the accuracy and reliability of gait biometric identification can be improved, ensuring that the technology is effective across diverse user populations.

While gait recognition technology offers the potential for secure and reliable authentication, it also raises privacy concerns. Biometric data, including gait patterns, is highly sensitive and unique to each individual. As such, future research must prioritize addressing privacy concerns and developing robust privacy protection mechanisms. This includes obtaining explicit consent from users to use their biometric data and ensuring that it is stored and processed securely. A comprehensive understanding of privacy implications is essential to foster public trust and acceptance of gait recognition technology.

When considering a cloud-based approach for gait recognition, the security of the cloud infrastructure becomes a critical aspect to address. Storing biometric data in the cloud introduces potential security vulnerabilities that can lead to data breaches or unauthorized access. Future research should focus on identifying and mitigating these risks by implementing strong encryption, access controls, and other security measures. By establishing a secure cloud environment, the integrity and confidentiality of biometric data can be preserved, ensuring the privacy and protection of individuals' sensitive information. Scalability is another important consideration for the adoption of a cloud-based gait recognition system, especially in the context of expanding smart home infrastructures. As the number of users and devices increases, the system

must be capable of handling heavy loads without compromising performance. Future research should evaluate the system's scalability by conducting rigorous testing under realistic conditions, simulating large-scale deployments. By identifying potential performance bottlenecks and optimizing the system's architecture, researchers can ensure that the cloud-based approach remains efficient and responsive even as the user base expands.

References

[1] F. K. Aldrich, "Smart Homes: Past, Present and Future," in *Inside the Smart Home*, R. Harper, Ed. London: Springer London, 2003, pp. 17–39.

[2] M. R. Alam, M. B. I. Reaz, and M. A. M. Ali, "A Review of Smart Homes—Past, Present, and Future," *IEEE Trans. Syst. Man Cybern. C Appl. Rev.*, vol. 42, no. 6, pp. 1190–1203, Nov. 2012.

[3] J. Higuera, A. Llenas, and J. Carreras, "Trends in smart lighting for the Internet of Things," *arXiv [cs.CY]*, 29-Aug-2018.

[4] I. Kastelan, M. Katona, G. Miljkovic, T. Maruna, and M. Vucelja, "Cloud enhanced smart home technologies," in *2012 IEEE International Conference on Consumer Electronics (ICCE)*, 2012, pp. 504–505.

[5] M. Jahn, M. Jentsch, C. R. Prause, F. Pramudianto, A. Al-Akkad, and R. Reiners, "The Energy Aware Smart Home," in *2010 5th International Conference on Future Information Technology*, 2010, pp. 1–8.

[6] M. Li, W. Gu, W. Chen, Y. He, Y. Wu, and Y. Zhang, "Smart home: architecture, technologies and systems," *Procedia Comput. Sci.*, 2018.

[7] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933–1954, Fourthquarter 2014.

[8] P. Kumar, "Design and implementation of Smart Home control using LabVIEW," in *2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*, 2017, pp. 10–12.

[9] S. Davidoff, M. K. Lee, C. Yiu, J. Zimmerman, and A. K. Dey, "Principles of Smart Home Control," in *UbiComp 2006: Ubiquitous Computing*, 2006, pp. 19–34.

[10] D. Valtchev and I. Frankov, "Service gateway architecture for a smart home," *IEEE Commun. Mag.*, vol. 40, no. 4, pp. 126–132, Apr. 2002.

[11] S. K. Das, D. J. Cook, A. Battacharya, E. O. Heierman, and T.-Y. Lin, "The role of prediction algorithms in the MavHome smart home architecture," *IEEE Wirel. Commun.*, vol. 9, no. 6, pp. 77–84, Dec. 2002.

[12] D. Marikyan, S. Papagiannidis, and E. Alamanos, "A systematic review of the smart home literature: A user perspective," *Technol. Forecast. Soc. Change*, vol. 138, pp. 139–154, Jan. 2019.

[13] M. Alaa, A. A. Zaidan, B. B. Zaidan, M. Talal, and M. L. M. Kiah, "A review of smart home applications based on Internet of Things," *Journal of Network and Computer Applications*, vol. 97, pp. 48–65, Nov. 2017.

[14] R. Kadam, P. Mahamuni, and Y. Parikh, "Smart home system," *International Journal of Innovative Research in Advanced Engineering*, vol. 2, no. 1, pp. 81–86, 2015.

[15] D. Ding, R. A. Cooper, P. F. Pasquina, and L. Fici-Pasquina, "Sensor technology for smart homes," *Maturitas*, vol. 69, no. 2, pp. 131–136, Jun. 2011.

[16] V. S. Gunge and P. S. Yalagi, "Smart home automation: a literature review," *Int. J. Comput. Appl. Technol.*, vol. 975, no. 8887–8891, 2016.

[17] R. D. Labati, A. Genovese, E. Muñoz, V. Piuri, F. Scotti, and G. Sforza, "Biometric Recognition in Automated Border Control: A Survey," *ACM Comput. Surv.*, vol. 49, no. 2, pp. 1–39, Jun. 2016.

[18] A. Saad al-sumaiti, M. H. Ahmed, and M. M. A. Salama, "Smart Home Activities: A Literature Review," *Electr. Power Compon. Syst.*, vol. 42, no. 3–4, pp. 294–305, Mar. 2014.

[19] A. K. Jain and A. Kumar, "Biometric Recognition: An Overview," in *Second Generation Biometrics: The Ethical, Legal and Social Context*, E. Mordini and D. Tzovaras, Eds. Dordrecht: Springer Netherlands, 2012, pp. 49–79.

[20] Z. Rui and Z. Yan, "A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification," *IEEE Access*, vol. 7, pp. 5994–6009, 2019.

[21] G. Demiris and B. K. Hensel, "Technologies for an Aging Society: A Systematic Review of 'Smart Home' Applications," *Yearb. Med. Inform.*, vol. 17, no. 01, pp. 33–40, 2008.

[22] R. J. Robles, T. Kim, D. Cook, and S. Das, "A review on security in smart home development," *International Journal of Advanced*, 2010.

[23] M. D. Marsico and A. Mecca, "A Survey on Gait Recognition via Wearable Sensors," *ACM Comput. Surv.*, vol. 52, no. 4, pp. 1–39, Aug. 2019.

[24] R. Katiyar, V. K. Pathak, and K. V. Arya, "A study on existing gait biometrics approaches and challenges," *International Journal of Computer Science*, 2013.

[25] T. K. M. Lee, M. Belkhatir, and S. Sanei, "A comprehensive review of past and present vision-based techniques for gait recognition," *Multimed. Tools Appl.*, vol. 72, no. 3, pp. 2833–2869, Oct. 2014.