How to improve the security and privacy of users in Cloud-based smart home systems?

Zhangyi Wu
University of Melbourne
zhangyiw1@student.unimelb.edu.au

Zitian Li
University of Melbourne
zitian1@student.unimelb.edu.au

Xiaojian Liu
University of Melbourne
xiaojianl@student.unimelb.edu.au

Jingman Zhuang
University of Melbourne
jingmanz@student.unimelb.edu.au

Junnan Ma
University of Melbourne
junnanm1@student.unimelb.edu.au

Rod Dilnutt
University of Melbourne
rpd@unimelb.edu.au

Abstract

As technology develops and demand grows, smart home systems, part of the Internet of Things (IoT), using Cloud services have been designed and adopted. Compared to traditional technologies such as Bluetooth, Cloud services can better help smart home systems expand their capacity and cater to demand. The existing three-layer architecture can integrate Cloud services and smart home systems to improve services.

However, Cloud services are more vulnerable, the root causes of which are investigated through case studies of voice assistants and home cameras in this report. Unreliability of Cloud service providers, and attacks from outside threats, makes smart home systems vulnerable to data leakage and network instruction, which violate users' privacy and can even cause serious harm to users and other stakeholders.

The purpose of this report is to analyse and deal with these issues in terms of cyber security when adopting Cloud-based smart home systems. To improve security, this report complements new elements to the original architecture, providing approaches covering blockchain, physical unclonable functions, and edge computing.

Keywords: Cloud-based smart home system, IoT, Security, Privacy, Data leakage, Data tampering, Blockchain, PUF, Edge computing

Acknowledegement

Heartfelt thanks to our research supervisor Dr. Rod Dilnutt and, academic tutor Dr. Leila Meratian and industry experts for invaluable guidance in this work. Gratitude to the University of Melbourne.

1. Introduction

As one of the applications of the Internet of Things (IoT), smart home systems, which encapsulate a lot of security data and private information, have become the target of cyber-attacks (Dorr et al., 2017). To improve the capability of management and operation, as well as achieve value-added services, the trend of integrating smart home systems and cloud technology has emerged (Lee et al., 2016). Consequently, the nature of cloud services, like shareability which may lead to malicious data control, has raised further concerns among users (Al Nafea & Almaia, 2021).

Negligence in the security of smart home systems may cause privacy violations, which bring serious consequences. On the one hand, the way to handle users' personal information is supervised by laws like Privacy Act 1988 at the legal level (Bygrave, 1990). Furthermore, if the user's data is compromised, the user may suffer a series of severe consequences, such as personal safety injury, financial loss, and mental trauma. On the other hand, for merchants, data leakage can increase customer dissatisfaction and seriously affect reputation, leading to loss of sales.

Based on the seriousness of the threats mentioned above, this report aims to dissect the reasons behind the cyber threat and then reinforce the existing framework of Cloud-based smart home systems. To fill the lack of existing literature and research on enhancing architecture from a security perspective, the research question posed in this report is:

"How do we improve the security and privacy of users in Cloud-based smart home systems?"

The following sections for context analysis and case studies of Cloud-based smart home systems will help to solve this problem.

2. Literature review

2.1 Context and elements of the smart home

The Internet of Things is an automated information processing technology that enables the interaction of two targets from smart sensor devices to information processing centers under a network connection (Liu & Lu, 2012). International Telecommunication Union (2005) demonstrated that the era of IoT has been coming since 2015 because various kinds of objects in daily life can be installed with smart sensors and interact with people or other systems.

Smart home is the most notable application in IoT. According to Jiang et al. (2004), the necessary elements of a smart home system are the internal network, home automation (links between products and systems), and intelligent control (shown in Figure1). The author also mentions that intelligent control is the gateway that represents the management system. Based on Alaa et al. (2017), the gateway refers to detection and control devices in smart homes, including switches and sensors. The classification of products in smart home systems with author information is shown in Table 1.

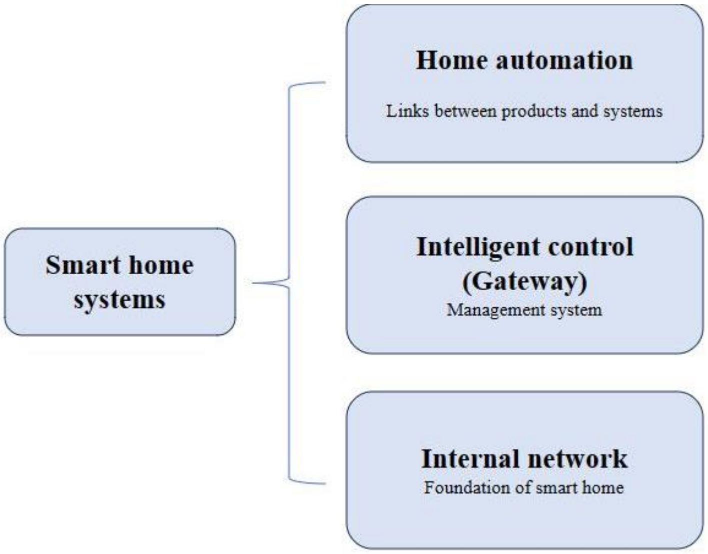

Figure1. Elements of smart home systems adapted from "Smart home research" Jiang et al., 2004

Basis of classification	Classification	Author
Applications	"Lighting, shading system , controlling of appliances, heating, ventilation and air conditioning (HVAC), safety functions, multimedia, health, kitchen, irrigation, cleaning, control"	P. Hamernik, P. Tanuska, Member, IACSIT, and D. Mudroncik (2012)
Functions	"Elderly / aging / home care, energy efficiency, comfort / entertainment, safety / security"	Costin Badic ˘ a, Marius Brezovan, Amelia Badic ˘ a (2013)

Table1. Classification of smart home products. Adapted from "Classification of functions in smart home" Hamernik et al., 2012 and "An Overview of Smart Home Environments" Badica et al., 2013.

2.2 Cloud-based smart home systems

The connectivity and control of smart home systems rely on different technologies, such as Bluetooth and local networks, which are well-known to the public and have been developed for years (Kumar et al., 2021). Nevertheless, as demand increases and product requirements rise, the relatively poor capability of connectivity no longer meets the needs of users and businesses. Smart homes based on Cloud services come into the picture with their most notable feature of carrying and handling large volumes of data (Kumar et al., 2021). In addition, Hanumanthaiah et al. (2019) and Iqbal et al. (2018) pointed out that using cloud technology has many benefits that cannot be achieved by traditional technologies, such as lower costs, improved interoperability, and providing backup for data.

2.3 Complementation for cloud technology

There are some additional methods that can complement the use of Cloud-based smart home systems with the aim of improving data security. According to Wu et al. (2022), embedding a Physical Unclonable Function (PUF) in the smart objectives can prevent data leakage attacks. Edge computing is distributed computing that can enhance real-time data processing capabilities (Kumar et al., 2021). Wu et al. (2022) also stated that applying anonymous authentication protocols covering edge computing to smart home environments can secure communication between entities. Based on Dorri et al. (2017) and Ren et al. (2021), lightweight, scalable, and distributed security is needed by IoT, and the distributed features of blockchain can enhance security and protect privacy for the smart home.

2.4 Cloud-based smart home architecture

According to Ye and Huang (2011), the three layers of the Cloud-based smart home are the infrastructure layer, platform layer, and service layer. Based on this, we created a cloud-based smart home architecture figure (show in Figure 2).

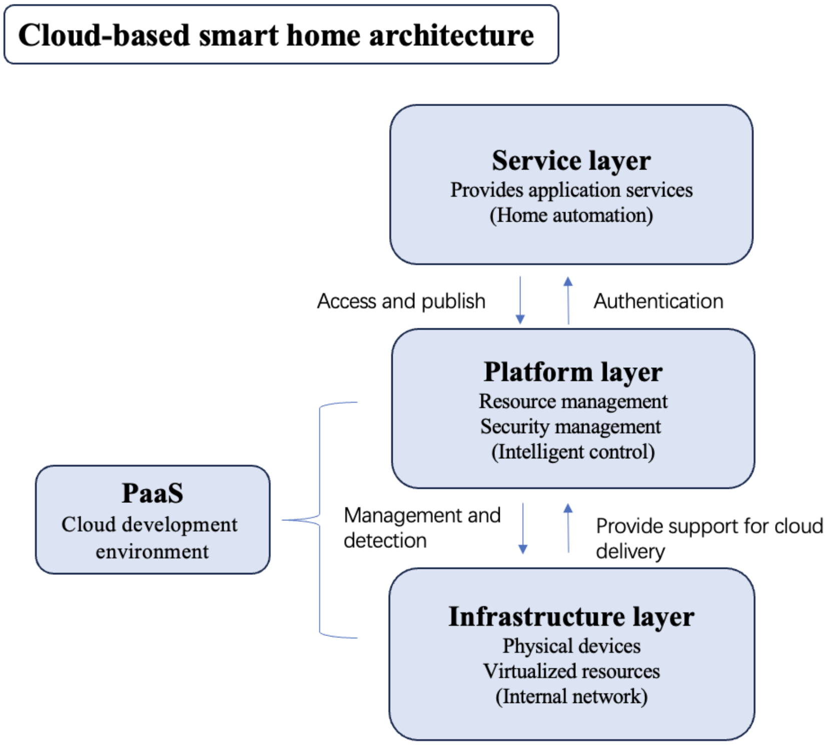

Figure 2. Cloud-based smart home architecture. Adapted from "A framework for Cloud-based. Smart Home" Ye and Huang (2011)

2.4.1 Infrastructure layer

The infrastructure layer is the lowest layer of the internal network and consists of physical and virtualised resources (Ye & Huang, 2011). Physical devices and hardware (e.g., servers and network components) are physical resources (Bhatia & Saggi, 2015). These physical resources are virtualised into a pool of resources through virtual machines (Bhatia & Saggi, 2015). The storage and computation of data, and other services are performed in the Cloud (Ali et al., 2022). In summary, this layer provides Cloud-based storage primarily for home devices, providing application service providers with the information they need (Iqbal et al., 2018). Users have access to remote hardware resources on demand (Yao et al., 2022).

2.4.2 Platform layer

The platform layer consists of resource management and security management, providing intelligent control for smart home systems (Ye & Huang, 2011). As the core middleware, it connects the application to the operating system (Wei et al., 2010). In addition, this layer manages the virtual resources of the infrastructure layer, for example, resource load balancing and detection of system status (Wei et al., 2010; Ye & Huang, 2011). This ensures compliance with service level agreements by coordinating resources in the Cloud (Yao et al., 2022). Security management ensures the security and stability of the Cloud environment, including user authentication and access restrictions, data security and reconfiguration (Wei et al., 2010; Ye & Huang, 2011).

In fact, the platform and infrastructure layers become the basis for providing Platform-as-a-Service (PaaS) for smart homes (Wei et al., 2010; Ye & Huang, 2011). Specifically, application developers can generate and maintain smart home programs directly on the platform (Bhatia & Saggi, 2015), combining different devices to implement customised smart home services (Ye & Huang, 2011). Hence, PaaS provides support for applications deployed on Cloud platforms by smart home providers (Yao et al., 2022).

2.4.3 Service layer

The service layer provides application services for smart home service providers and users (Ye & Huang, 2011). This layer presents home automation, which consists of interface, control, and directory (Wei et al., 2010). Service providers use APIs to create smart home services (e.g., remote control, audio or video communication) and register them in a service directory (Ye & Huang, 2011). Users search for and consume these services in a simple interface, which is handled and responded to by service controls (Wei et al., 2010).

Based on the above, the characteristics of the Cloud such as sharing resources, accommodating heterogeneity, and large storage capacity enable the smart home to better respond to user needs (Tao et al., 2018). Users can access data and operate home systems through the Cloud without the need for additional physical storage (Ye & Huang, 2011).

2.5 Security and privacy in Cloud-based smart home

Privacy and security issues in the smart home Cloud can affect human health and operational security (Tao et al., 2018). The complexity of Cloud models and sharing causes several issues (Flexera, 2020). For example, the combination of different devices in the Cloud raises security vulnerabilities (Parast et al., 2022). Cyber-attacks lead to denial of service or malicious control, breach of promises and laws by manufacturers. Cloud failures trigger response time failures (Merino-R et al., 2012). In addition, data storage in the Cloud is distributed and many dispersed data interactions may result in data loss and unauthorised access (Imran et al., 2017). These Cloud security issues may be projected into smart home systems, causing some security incidents (Ryan Heartfield). Therefore, a risky Cloud environment is not safe for users (Merino-R et al., 2012).

2.6 Case analysis

Although smart homes improve the lifestyle of people and bring comfort and convenience, the security and privacy of users are also at risk of being violated (Ali et al., 2017). Identification of digital hazards associated with smart homes has become essential with the rise in popularity of Cloud-based home devices.

2.6.1 Case in Cloud-based smart home system

Currently most voice assistants accompany us through smartphones and smart speakers, where users give commands through natural language which in turn are executed as commands like turning on the lights, TV, and playing music (Kudina & Coeckelbergh, 2021).

The spread of voice assistants is staggering. According to a survey, about 36 percent of American adults have a home voice assistant in 2020 (Kudina & Coeckelbergh, 2021). The insecurity of voice assistants is also emerging and generating widespread social discussion. According to Lynskey (2019), in 2017 Alexa (the nickname of the Amazon-owned voice assistant) was found to ask a user to re-book train tickets on a schedule he had already travelled. This means that Alexa is collecting user data indiscriminately. Coincidentally, the BBC also reported on a couple in Portland, Oregon, whose conversation was intercepted by Alexa and randomly sent to a contact (Lee, 2018). In fact, due to the complexity of language systems, most intelligent voice systems work on a Cloud-based platform, which is why they can easily collect and exploit data from users and even allow hackers to eavesdrop (Lynskey, 2019). Boukharrou et al. (2021) also mentioned that home assistants are storing enormous amounts of data in Cloud servers, and the privacy of users is being violated due to unreliable Cloud providers.

The voice assistant is part of the smart home and may become the central operating platform, its security rise is critical. Conversations being collected may be only a small part of the risk. If a Cloud-based voice assistant can be maliciously manipulated to open a door and allow a burglary to be committed, or the temperature of a thermostat modified, both people and assets will be at significant risk.

Increasingly, homes are installing home-surveillance cameras. Wired and wireless cameras are expected to grow at a CAGR of nearly 19% from 2023 to 2030 (Smart Home Security Cameras Market Size Report, 2020-2027, n.d.). Identifying the potential risks of Cloud-based home cameras is important. Surveillance cameras have a Pan-Tilt-zoom feature, whose main purpose is to adjust the view and zoom of the camera (Pan, 2019). The mobile application will help the user to view the live video stream from the camera while the PTZ requests are routed to the camera through the Cloud server. When the user uses the mobile application to view the live video stream from the camera, the PTZ requests are routed to the camera through the Cloud server (Vennam et al., 2021). The attacker has the opportunity to intercept the request and decode the video data and control the view (Vennam et al., 2021). This means that private cameras may become online livestream cameras (Buil-Gil et al., 2023).

2.6.2 The Cloud threat and impact in smart home

Potential threats in the Cloud can be exploited and applied to the smart home. Hacker attacks and unreliable Cloud providers have an impact on the privacy and well-being of the occupants and also create a threat to the safety of life and property. In the near future, smart homes are expected to appear in every aspect of human life (Ferreira et al., 2023). Hence, to improve security, it is a basic requirement to assess the potential risks, vulnerabilities, and critical threats of the system (Ali & Awad, 2018). There is a series of possible threats including 1.data loss 2. account hijacking 3. data control 4. malicious insider (Nafea & Amin Almaiah, 2021).

"A consequence of technology convergence in the smart home is the cascading effect of compromise of one system to others" (Heartfield et al., 2018, p. 399). Because of the special qualities of the Cloud environment cascading effects may project weaknesses of the Cloud into the smart home system.

There are six weakness of Cloud: One side about security, including virtualisation and hypervisor, data and storage, and network; the others are identity and access management, legal and compliance issues, and governance (Islam et al., 2016).

Identifying risks helps to avoid suffering adverse effects while warning of the importance of improving system security. The risks associated with the unsafety of Cloud-based smart home are 1. Privacy breaches (including data, video and voice leakage) 2. property damage 3. personal safety, which brings further risks of: 1. anxiety 2. stress 3. insecurity (Heartfield et al., 2018).

3. Cybersecurity Challenges for smart-home systems

Based on the security risks and privacy concerns in the earlier section, we discern three primary challenges through the evaluation of each layer of the ITS architecture. These are data breach issues and device takeovers instigated by external attackers, and insider threats emanating from unsecured Cloud service providers. The analysis reveals that all these challenges simultaneously exert a direct or indirect influence on all three layers of the architecture.

3.1 External Attackers

According to Sunehra and Bano (2014), Cloud-based smart home security systems have gained significant traction in recent years, offering homeowners the ability to monitor their properties remotely through internet-enabled devices. These systems often utilise IP webcams and mobile devices to capture images and videos, which can be stored in a public Cloud for later use. While preliminary experiments have shown promising results, there are several challenges associated with Cloud-based smart home security systems that must be addressed.

Utilising IP addresses in smart home security creates potential issues by making devices vulnerable to cyber threats. Hackers may take advantage of system flaws to access IP cameras without permission, view live streams, alter data, or even disable devices. This jeopardises homeowner security and privacy. The normal functioning of the service layer is disrupted, which could lead to the process of smart home service outages. The availability of the application and operating system would be affected. In addition, hackers could steal the storage and computation of sensitive data from the infrastructure layer if they gain access to the service layer. They can also potentially manipulate the data or leak it, causing harm to the organization and its users.

To reduce risk, it is essential to employ strong encryption, authentication, and frequent software updates, safeguarding devices from cyber-attacks and maintaining a secure home environment.

3.2 Insider threats

Cloud service providers' transition tasks to a communal infrastructure amplify the risk of unauthorised access and exposure to customers' confidential data. Cloud service providers are obligated to ensure their customers' trust by providing a significant level of transparency regarding their operations and privacy safeguards (Takabi et al., 2010). Otherwise, unreliable Cloud providers could potentially create a serious cyber threat from inside. Samia Bouzefrane et al. (2021) illustrate that the home assistant can store a large amount of data it collects on-site or remotely on Cloud servers. Unreliable Cloud providers may commit privacy violations against their customers by selling or otherwise exploiting the information they collect for profiling purposes. It makes it difficult to develop software for such devices that uses encrypted data and has a black-box appearance.

In the ITS architecture, both the infrastructure and platform layers need to consider security approaches and privacy mechanisms to protect against both inadvertent human errors and malicious insiders. The insider who takes advantage of a flaw in the infrastructure layer of a Cloud system to steal data, could take valuable data without permission, engage in fraudulent activities for financial gain, or publicly reveal confidential information. Alternatively, an insider might exploit Cloud technologies to launch an assault on an employer's in-house resources, which exposes the smart home programs in the platform layer and the smart home systems of the service layer to risk.

4. Security and privacy protection framework for smart home systems

With the development of IoT, more and more smart home systems realize remote control and data processing through Cloud services. Smart homes have become a typical device in modern homes. While bringing great convenience to users, it also brings security and privacy issues affecting people's lives (Yang & Sun, 2022). Wei et al. (2016) demonstrates that security issues in IoT systems and applications are becoming increasingly important and may hinder the spread of IoT application deployments or cause significant property damage due to security vulnerabilities. To solve this problem, Cloud-based smart home systems need to take some measures to improve the security and privacy of users. Based on the smart home Cloud architecture mentioned earlier in this report and several studies, it is suggested to enhance the security and privacy of smart home systems from three perspectives: blockchain, physical unclonable function (PUF), and edge computing (Figure 3).

4.1 Blockchain

Security and privacy on the IoT remain a significant challenge, mainly due to intelligent devices' complex, contemporary and diverse needs, and the need for distributed, transparent, and dynamic access to smart home systems. Lhore et al. (2023) mention that Blockchain is an innovative technology that assures information privacy, immutability, integrity, and availability while creating a distributed and decentralized system that is independent of other parties. Blockchain's anonymity, openness, non-repudiation, and consensus mechanisms can ensure the security of this access mode while also providing interoperability, decentralization, security, privacy protection, consistency, and continuity, which can increase the security of smart home systems (Yang & Sun, 2022).

The blockchain (BC) technology that supports Bitcoin is the first cryptocurrency system, which has the characteristics of distribution, security, and privacy and can provide decentralised security and privacy for the IoT based on the blockchain approach (Dorri et al., 2017). Therefore, the implementation of blockchain technology in the infrastructure, platform, and service layer of the smart home system can record all the data exchange in the Cloud to ensure that the data is not tampered with or stolen in the transmission process and record the authorised equipment and operations to ensure the privacy and security of users.

4.2 Physical unclonable functions (PUF)

In the smart home system, devices can be authenticated using a physical unclonable function (PUF), and communications can be encrypted to ensure user security and privacy. Physical non-cloning generates unique keys and identifiers based on the randomness and unpredictability of chips, providing more secure authentication and encryption (Suh & Devadas, 2007; Durand & Pasquier, 2021). In addition, Wu et al. (2022) proposed that applying PUF technology to intelligent devices can prevent attackers from launching data leakage attacks, protect data security, and resist tampering and biological cloning attacks. Therefore, since the keys and identifiers generated by the PUF cannot be copied and forged, applying PUF technology in the infrastructure layers of smart home systems can prevent unauthorised devices from accessing the system and its data, thus preventing attackers from obtaining sensitive user information.

4.3 Edge-computing

As a new computing paradigm, edge-computing provides a new solution for the design and deployment of security and privacy of smart home systems. Edge computing allows people to stay anonymous and private (Lopez et al., 2015). According to Shi et al. (2016), edge computing, as an extension of the Cloud, moves massive computational and storage capabilities to the network's edge, providing an edge layer close to IoT terminal devices. Edge computing has more resources than IoT terminal devices and can support computation-intensive security operations like homomorphic encryption and attribution-based access control (Sha et al., 2019). Thus, in smart home systems, computation-heavy and memory-demanding operations can be performed on the edge layer to limit data transmission and storage in the Cloud, lowering the risk of data leakage or hacking. Furthermore, some IoT security solutions include edge computation-based security architectural designs such as firewalls, intrusion detection systems, authentication and authorisation protocols, and privacy protection methods (Sha et al., 2019). Therefore, the security and privacy of smart home systems can be improved by using edge computing in the platform layer of smart home systems, as it can process data locally on the device and reduce Cloud data transmission.

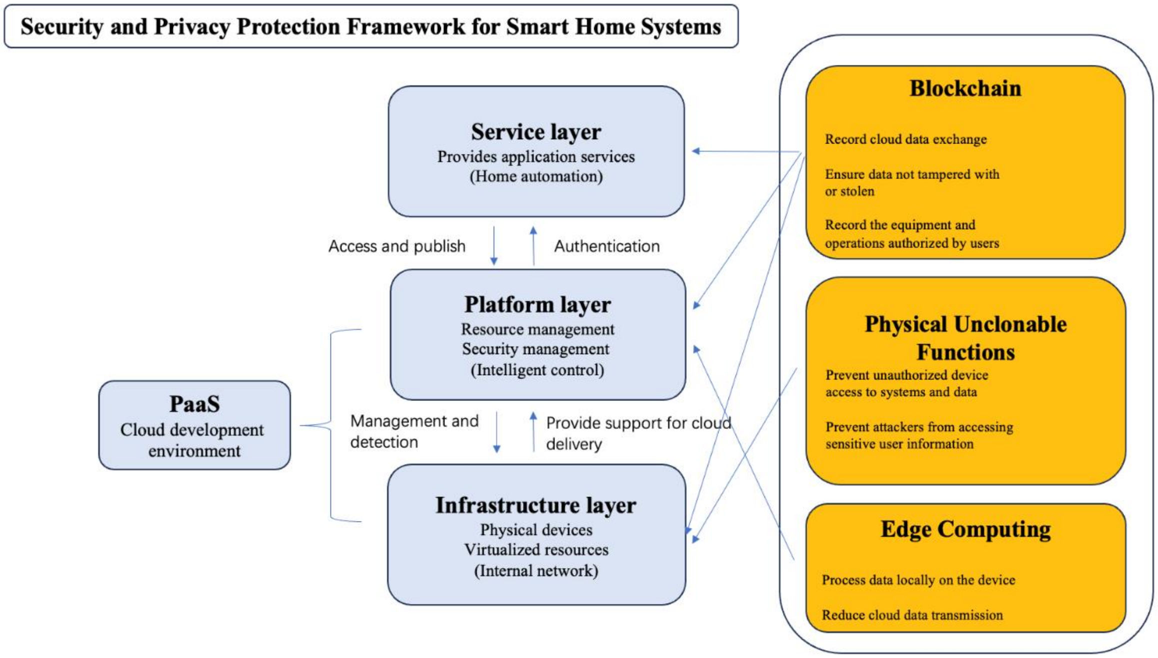
Security and Privacy Protection Framework for Smart Home Systems
Service layer
Provides application services
(Home automation)
Access and publish
Authentication
Platform layer
Resource management
Security management
(Intelligent control)
PaaS
Cloud development environment
Management and detection
Provide support for cloud delivery
Infrastructure layer
Physical devices
Virtualized resources
(Internal network)
Blockchain
Record cloud data exchange
Ensure data not tampered with or stolen
Record the equipment and operations authorized by users
Physical Unclonable Functions
Prevent unauthorized device access to systems and data
Prevent attackers from accessing sensitive user information
Edge Computing
Process data locally on the device
Reduce cloud data transmission

Figure 3. Security and privacy protection framework for smart home systems. Adapted from"A framework for Cloud-based. Smart Home" Ye and Huang (2011)

5. Limitations

The report focuses on the Cloud-based smart home architecture but does not mention the layers of smart homes only based on IoT. It discusses the main challenges of smart homes based on the Cloud and analyses their impact on different layers. However, it does not mention other challenges of smart homes based in the Cloud, such as heterogeneity and latency. These are two vital elements that contribute to overall efficacy, user-friendliness, and satisfaction of the end-user but are not within the scope of the topic discussed in the text. Furthermore, fog computing is not mentioned or discussed in the context of the document. Although both Cloud computing and fog computing offer advantages, Cloud computing may be preferred for a smart home setup.

6. Conclusion

As Cloud-based smart home systems become more and more common in people's lives, some studies have shown that they have attracted considerable attention in terms of data security and user privacy protection. To improve the security and privacy of users, this report first mentions that the Cloud-based smart home architecture is the infrastructure layer, platform layer and service layer. This report also compares and analyses several cases of smart home systems and describes in detail some threats and potential risks brought by Cloud computing to smart home systems, which are accompanied by some limitations and challenges. Finally, according to the architecture of the smart home system, it is proposed to use blockchain technology, physical unclonable functions and edge computing to help the smart home system solve the user's security and privacy issues.

References

Al Nafea, R., & Almaiah, M. A. (2021). Cyber security threats in cloud: Literature review. In *2021 International Conference on Information Technology (ICIT)* (pp. 779-786). IEEE. https://doi.org/10.1109/ICIT52682.2021.9491638

Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M. (2017). A review. of smart home applications based on Internet of Things. *Journal of Network and Computer Applications*, 97, 48-65. https://doi.org/10.1016/j.jnca.2017.08.017

Ali, B., & Awad, A. (2018). Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors*, *18*(3), 817. https://doi.org/10.3390/s18030817

Ali, M., Tang Jung, L., Hassan Sodhro, A., Ali Laghari, A., Birahim Belhaouari, S., & Gillani, Z. (2022). A Confidentiality-based data Classification-as-a-Service (C2aaS) for cloud security. *Alexandria Engineering Journal*, *64*. https://doi.org/10.1016/j.aej.2022.10.056

Ali, W., Dustgeer, G., Awais, M., & Shah, M. A. (2017). IOT based Smart Home: Security. Challenges, security requirements and solutions. *2017 23rd International Conference on Automation and Computing (ICAC)*. https://doi.org/10.23919/iconac.2017.8082057

Badica, C., Brezovan, M., & Badica, A. (2013). An Overview of Smart Home Environments: Architectures, Technologies and Applications. *BCI (Local)*, *78*.

Bhatia, A. S., & Saggi, M. K. (2015). A Review on Mobile Cloud Computing: Issues, Challenges and Solutions. *International Journal of Advanced Research in Computer and Communication Engineering*, *4*(6), 29–30. https://doi.org/10.17148/IJARCCE.2015.4608

Boukharrou, R., Chaouche, A. C., & Mahdjar, K. (2021). Toward a Privacy Guard for Cloud. Based Home Assistants and IoT Devices. *Mobile, Secure, and Programmable Networking*, *12605*, 177–194. https://doi.org/10.1007/978-3-030-67550-9_12

Buil-Gil, D., Kemp, S., Kuenzel, S., Coventry, L., Zakhary, S., Tilley, D., & Nicholson, (2023). The digital harms of Smart Home Devices: A systematic literature review. *Computers in Human Behavior*, *145*, 107770. https://doi.org/10.1016/j.chb.2023.107770

Bygrave, L. A. (1990). The Privacy Act 1988 (Cth): A study in the protection of privacy and the protection of political power. *Federal Law Review*, *19*(2), 128-153. https://doi.org/10.1177/0067205X9001900203

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and. privacy: The case study of a smart home. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* (pp. 618-623). IEEE. https://doi.org/10.1109/PERCOMW.2017.7917634

Durand, A., & Pasquier, J. (2021, November). Physical Unclonable Functions for IoT. Security using Free Software. *IoT '21: Proceedings of the 11th International Conference on the Internet of Things* [Symposium].

Ferreira, L., Oliveira, T., & Neves, C. (2023). Consumer's intention to use and recommend. smart home technologies: The role of environmental awareness. *Energy*, *263*(C), 125814. https://doi.org/10.1016/j.energy.2022.125814

Hamernik, P., Tanuska, P., & Mudroncik, D. (2012). Classification of functions in smart home. *International Journal of Information and Education Technology*, *2*(2), 149-155. https://doi.org/10.7763/IJIET.2012.V2.98

Hanumanthaiah, A., Arjun, D., Liya, M. L., Arun, C., & Gopinath, A. (2019). Integrated cloud. based smart home with automation and remote controllability. In *2019 International Conference on Communication and Electronics Systems (ICCES)* (pp. 1908-1912). IEEE. https://doi.org/10.1109/ICCES45898.2019.9002245

Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J. R. J., Filippoupolitis, A., & Roesch, E. (2018). A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security*, *78*, 398–428. https://doi.org/10.1016/j.cose.2018.07.011

Imran, M., Hlavacs, H., Haq, I. U., Jan, B., Khan, F. A., & Ahmad, A. (2017). Provenance based data integrity checking and verification in cloud environments. *PLOS ONE*, *12*(5), e0177576. https://doi.org/10.1371/journal.pone.0177576

International Telecommunication Union. (2005). ITU Internet Reports 2005: The internet of things (1st ed., p. 62). Geneva: International Telecommunication Union.

Iqbal, A., Ullah, F., Anwar, H., Kwak, K. S., Imran, M., Jamal, W., & Rahman, A. ur. (2018). Interoperable Internet-of-Things platform for smart home system using Web-of-Objects and cloud. *Sustainable Cities and Society*, *38*, 636–646. https://doi.org/10.1016/j.scs.2018.01.044

Islam, T., Manivannan, D., & Zeadally, S. (2016). A classification and. characterization of security threats in cloud computing. Int. J. Next-Gener. *Comput*, 7(1), 268-285.

Jiang, L., Liu, D. Y., & Yang, B. (2004). Smart home research. In *Proceedings of 2004 international conference on machine learning and cybernetics (IEEE Cat. No. 04EX826)* (Vol. 2, pp. 659-663). IEEE. https://doi.org/10.1109/ICMLC.2004.1382266

Kudina, O., & Coeckelbergh , M. (2021). "Alexa, define empowerment": Voice assistants at. home, appropriation and technoperformances. *Journal of Information, Communication & Ethics in Society*, *19*(2), 299-312. https://doi.org/10.1108/JICES-06-2020-0072

Kumar, U., Verma, P., & Abbas, S. Q. (2021). Critical analysis of challenges facing with cloud computing based iot and techniques used to improve quality of service. In *2021 6th International Conference on Communication and Electronics Systems (ICCES)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICCES51350.2021.9489256

Lee, D. (2018, May 24). Amazon Alexa heard and sent private chat. *BBC News*. https://www.bbc.com/news/technology-44248122

Lee, Y. T., Hsiao, W. H., Huang, C. M., & Seng-cho, T. C. (2016). An integrated cloud-based smart home management system with community hierarchy. *IEEE Transactions on Consumer Electronics*, *62*(1), 1-9. https://doi.org/10.1109/TCE.2016.7448556

Lhore, H., Bousselam, K., Elissati, O., & Chami, M. (2023). Blockchain Technology. as a Possible Solution to IoT Security Issues. *International Journal of Engineering Trends and Technology, 71(1),* 152–163. https://doi.org/10.14445/22315381/ijett-v71i1p214

Liu, T., & Lu, D. (2012, August). The application and development of IoT. In *2012 International symposium on information technologies in medicine and education* (Vol. 2, pp. 991-994). IEEE. https://doi.org/10.1109/ITiME.2012.6291468

Lopez, P., Montresor, A., Epema, D., Datta, A., Higashino, T., Iamnitchi, A., Barcellos, M. P., Felber, P., & Rivière, E. (2015). Edge-centric Computing. *Computer Communication Review, 45(5),* 37–42. https://doi.org/10.1145/2831347.2831354

Lynskey, D. (2019, October 9). *"Alexa, are you invading my privacy?" – the dark side of our voice assistants*. The Guardian; The Guardian. https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants

Mocrii, D., Chen, Y., & Musilek, P. (2018). IoT-based smart homes: A review of. system architecture, software, communications, privacy and security. *Internet of Things, 1–2,* 81–98. https://doi.org/10.1016/j.iot.2018.08.009

Nafea, R. A., & Almaiah, M. A. (2021). Cyber security threats in cloud: Literature review. *2021 International Conference on Information Technology (ICIT),* 799–786. https://doi.org/10.1109/icit52682.2021.9491638

Pan, J. (2019). Physical Integrity Attack Detection of Surveillance Camera with Deep Learning based Video Frame Interpolation. *2019 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*. https://doi.org/10.1109/iotais47347.2019.8980385

Parast, F. K., Sindhav, C., Nikam, S., Yekta, H. I., Kent, K. B., & Hakak, S. (2021). Cloud Computing Security: A Survey of Service-based Models. *Computers & Security, 114*, 102580. https://doi.org/10.1016/j.cose.2021.102580

Ren, Y., Leng, Y., Qi, J., Sharma, P. K., Wang, J., Almakhadmeh, Z., & Tolba, A. (2021). Multiple cloud storage mechanism based on blockchain in smart homes. *Future Generation Computer Systems, 115,* 304-313. https://doi.org/10.1016/j.future.2020.09.019

Rodero-Merino, L., Vaquero, L. M., Caron, E., Muresan, A., & Desprez, F. (2012). Building safe PaaS clouds: A survey on security in multitenant software platforms. *Computers & Security*, *31*(1), 96–108. https://doi.org/10.1016/j.cose.2011.10.006

Samia Bouzefrane, Maryline Laurent, Boumerdassi, S., Renault, E., & Springerlink. (Online Service. (2021). *Mobile, Secure, and Programmable Networking: 6th International Conference, MSPN 2020, Paris, France, October 28{u2013}29, 2020, Revised Selected Papers*. Springer International Publishing.

Sha, K., Wei, W., Yang, T., Wang, Z., & Shi, W. (2018). On security challenges and. open issues in Internet of Things. *Future Generation Computer Systems, 83,* 326–337. https://doi.org/10.1016/j.future.2018.01.059

Sha, K., Yang, T., Wei, W., & Davari, S. (2019). A survey of edge computing-based. designs for IoT security. *Digital Communications and Networks, 6(2),* 195–202. https://doi.org/10.1016/j.dcan.2019.08.006

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge Computing: Vision and. Challenges. *IEEE Internet of Things Journal, 3(5),* 637–646. https://doi.org/10.1109/jiot.2016.2579198

Smart Home Security Cameras Market Size Report, 2020-2027. (n.d.). Www.grandviewresearch.com. https://www.grandviewresearch.com/industry-analysis/smart-home-security-camera-market

Suh, G. E., & Devadas, S. (2007). Physical Unclonable Functions for Device. Authentication and Secret Key Generation. In IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/4261134

Sunehra, D., & Bano, A. (2014). An intelligent surveillance with cloud storage for. home security. *2014 Annual IEEE India Conference (INDICON)*. https://doi.org/10.1109/indicon.2014.7030567

Takabi, H., Joshi, J. B. D., & Ahn, G.-J. (2010). Security and Privacy Challenges in. Cloud Computing Environments. *IEEE Security & Privacy Magazine*, *8*(6), 24–31. https://doi.org/10.1109/msp.2010.186

Tao, M., Zuo, J., Liu, Z., Castiglione, A., & Palmieri, F. (2018). Multi-layer cloud. architectural model and ontology-based security service framework for IoT-based smart homes. *Future Generation Computer Systems*, *78*, 1040–1051. https://doi.org/10.1016/j.future.2016.11.011

Vennam, P., T. C., P., B. M., T., Kim, Y.-G., & B. N., P. K. (2021). Attacks and Preventive. Measures on Video Surveillance Systems: A Review. *Applied Sciences*, *11*(12), 5571. https://doi.org/10.3390/app11125571

Wei, W., Yang, A., & Shi, W. (2016). Security in Internet of Things: Opportunities and Challenges. In International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI). IEEE. https://doi.org/10.1109/iiki.2016.35

Wei, Z., Qin, S., Jia, D., & Yang, Y. (2010). Research and design of Cloud. architecture for smart home. *2010 IEEE International Conference on Software Engineering and Service Sciences*. https://doi.org/10.1109/icsess.2010.5552297

Wu, T., Kong, F., Wang, L., Chen, Y., Kumari, S., & Pan, J. (2022). Toward Smart Home Authentication Using PUF and Edge-Computing Paradigm. *Sensors, 22(23),* 9174. https://doi.org/10.3390/s22239174

Xiaojing Ye, & Junwei Huang. (2011, December 1). *A framework for Cloud-based. Smart Home*. IEEE Xplore. https://doi.org/10.1109/ICCSNT.2011.6182105

Yang, J., & Sun, L. (2022). A Comprehensive Survey of Security Issues of Smart Home System: “Spear” and “Shields,” Theory and Practice. *IEEE Access, 10,* 124167–124192. https://doi.org/10.1109/access.2022.3224806

Yao, W., Wang, Z., Hou, Y., Zhu, X., Li, X., & Xia, Y. (2023). An energy-efficient. load balance strategy based on virtual machine consolidation in cloud environment. *Future Generation Computer Systems*, *146*, 222–233. https://doi.org/10.1016/j.future.2023.04.014