Prevention of IoT-Enabled Crime Using Home Routers (PITCHR)

Mary Asante(✉), Carsten Maple, and Gregory Epiphaniou

Secure Cyber Systems Research Group, WMG, University of Warwick, Coventry CV4 7AL, UK
mary.asante.1@warwick.ac.uk

Abstract. The home router has traditionally been the access point for home users to access email and web services through a desktop computer but has now become the entry point for a myriad of Internet-connected devices. With nearly all households in Europe having high-speed broadband connection, home routers have become targets for most cyber-attacks. This paper presents the findings of a study on the Prevention of IoT-enabled Crime using Home Routers (PITCHR). The study aims to understand the perspectives of the major stakeholders of the home router network in PITCHR, their respective roles and responsibilities, and make recommendations for future research directions. To achieve this, we conducted a review of state of the art, which informed a series of focus group discussions, with 26 participants from the respective stakeholder groups – Service Providers including Internet Service Providers, Hardware Manufacturers, Citizens, Citizen and Industry Groups, Government and Academics. Ten (10) themes emerged from the thematic coding of the focus group discussions. The findings of the study were presented in a combined stakeholder workshop. The study made recommendations for consideration.

Keywords: Home routers · IoT-enabled crime · Consumer IoT · Internet Service Providers · Home network

1 Introduction

Home-based routers are becoming increasingly integral parts of our way of life, with homes becoming smarter and devices connecting to each other [1]. Having traditionally been the access point for home users to access email and web services through a desktop computer, they are now becoming the entry point for a myriad of Internet-connected devices. These include smart assistants (e.g. Amazon Echo and Google Home), smart wearables (e.g. Fitbit), smart security (e.g. Ring and baby monitors), smart appliances (e.g. smart kettles, fridges and washing machines), smart energy (e.g. Nest and smart plugs) and many more. As such, the router becomes a gateway to a significant number of devices, considerable computing power and a variety of personal information, present challenges [2], which can be exploited with minimal effort [3].

S. Paiva et al. (Eds.): SmartCity360° 2021, LNICST 442, pp. 470–481, 2022.
https://doi.org/10.1007/978-3-031-06371-8_31

Eurostat reported that in 2020, nearly all households in Europe had been switched to high-speed broadband connection, an estimated 91% of households in the EU 27 and 97% in the UK [4]. However, as highlighted by the German Federation Office for Information Security in their requirements for secure broadband routers, "At the same time the number of devices per household that uses or even requires Internet access to be fully functional increases. This trend is predicted to continue and leads to more and more everyday things being equipped with networking and Internet capabilities" [5]. As a result, the nature of the threats that the home router network faces are constantly changing as new risks are being introduced all the time at a very fast pace.

Additionally, a study conducted by Germany's Fraunhofer Institute for Communication (FKIE) analysed over 127 home routers manufactured by top brands, including ASUS, Netgear, D-Link, TP-Link and Linksys, and found that all the home routers have security flaws. Also, 46 home routers had not been updated once within the previous 12 months and had weak passwords which could easily be cracked that users could not change. They also found that 22 home routers were from top vendors had not been updated in two years, and dozens had not received any security update in the past year [6]. These flaws leave home users widely opened and vulnerable to existing and emerging cyber security threats. Moreover, end users are not receiving sufficient information about their devices' security features from manufacturers [7].

The remainder of the paper is structured as follows: Sect. 2 presents the methodology used to collect and analyse the focus groups responses. Section 3 presents the critical analysis of the results. Section 4 presents the key findings and Sect. 5 makes recommendations. Finally, Sect. 6 concludes this paper.

2 Methodology

2.1 Background of This Study

Three key stakeholder focus group discussions were undertaken with industry and security experts to understand the roles that Service Providers, Hardware and Hardware Manufactures and Citizens and Citizen groups play in PITCHR. The focus group discussions offered insights into the various stakeholders' perspectives and the challenges faced by each of these stakeholders in the prevention of IoT-enabled crime using home routers. These include each stakeholder's role in PITCHR, how technology can reduce the impact of future crime and whom the responsibility and the financial burden lies with. A follow-on combined stakeholder workshop was conducted with participants from all stakeholder groups to discuss the findings of the study.

2.2 Participants

Each session had representatives from leading organisations and industry experts such as Cisco, Vonage, BT, and representation from government agencies such as the UK Home Office and National Cyber Security Centre (NCSC). There was an average of 12 participants per session. The sessions were very interactive and provided opportunities for in-depth discussions on the role of:

- Service Providers (Internet Service Providers (ISPs) eg BT, Virgin, TalkTalk etc. and other Service Providers such as Google, Amazon, Microsoft, and payment providers eg Mastercard).
- Hardware and hardware manufacturers such as Linksys and D-Link and IoT device manufacturers.
- Citizens and citizen groups such as Which and Consumer International. In this session, we also explored the roles of organisations such as IoTSF (Internet of Things Security Foundation) and Messaging Anti Abuse Working Group (MAAWG).
- Government, legislation, and standards.

2.3 Procedure

Each focus group discussion lasted 90 min. A sample of the questions used is presented in Table 1. The recordings for each of the sessions were transcribed. The researchers read and re-read through the transcripts to identify potential themes. The researchers used thematic analysis to identify initial codes, which were reviewed and refined to determine the main themes and sub-themes. The themes were shaped by the research topic, Prevention of IoT-enabled Crime using Home Routers (PITCHR) and the literature review conducted as part of the study. Ten main themes were identified as presented in Table 2.

Table 1. Sample Questions for the Focus Group Discussions.

Session 1	Session 2	Session 3
1. How have you seen home router technology evolve over the past decade; how has the role of Service Providers evolved in terms of providing home router security?	How have you seen home router technology evolve over the past decade; how has the role of hardware manufacturers evolved in terms of providing home router security?	To what extent are you aware of the scale of security threats to home router security?
2. Which tools and techniques are you are of that Service Providers are currently using to ensure security of home routers?	Which tools and techniques are you are of that hardware manufacturers are currently using to ensure the security of home routers?	How much responsibility is placed on the individuals in ensuring the security of their home router?
3. In your opinion, how much does it cost Service Providers to currently provide home router defence systems?	Which Tools and techniques can hardware manufacturers deploy and/or enhance to improve home router security?	How sensitive are consumers to paying more for their services for use towards home router security enhancement/improvement?

Table 2. Emergent Themes.

Code	Theme
1	Evolution of Home Router Technology
2	Future of Router Technology
3	The Role of Service Providers
4	The Role of Hardware and Hardware Manufacturers
5	The Role of Citizen and Industry Groups
6	Cost of Providing Home Router Security
7	Regulatory Role and Impact
8	Who is / should be Responsible for Home Router Security
9	User Awareness and Education
10	Changing Nature of Home Router Cyber Security Landscape

3 Results

3.1 Evolution of Home Router Technology

Routers were created as a result of technological research and development in compliance with IEEE802.11, allowing for the wireless transfer of data between devices. They were subsequently made available to home users in 1999, coincidentally, the same year that Kevin Ashton coined the term 'Internet of Things' [8]. Home routers provide internet access for devices on the home network such as wearable devices, smart assistants, gaming systems, mobile devices and smart appliances, as illustrated in Fig. 1. Most homes use wireless routers, although some homes, still use wired routers, using Ethernet cables to connect devices to the routers.

Home routers were very simple and basic, without many features on them. However, all the participants agreed that they have since become a lot more sophisticated over the years, offering many more capabilities, faster speeds, and generally have become more powerful. For example, they incorporate firewall technologies that filter the inflow and set up guest networks in the home, allowing for segregation of traffic on the home network.

New Customer Premise Equipment (CPE) operate pretty much like computers with powerful cores and processors and improved performance [9]. Moreover, in most cases, software capability allowing customisation on the CPE may not be enabled upon delivery to the end-user, thus limiting the CPE's capability. Some of the significant security posture changes are better wireless encryption technology, mandatory password requirements on devices, and enforcing specific initial set up rules for devices.

Routers can automate updates of firmware and software, execute security patches, and block out bad sites to the extent that the end-users are not even aware of what happens in their routers. Home users can configure their home router network to suit their needs. For example, they can set a downtime for the router when it goes to sleep for a set period. Home users can isolate devices off their network and can see the list

of devices connected to their network. Home routers can be configured through apps, making it easier for home users to control their network.

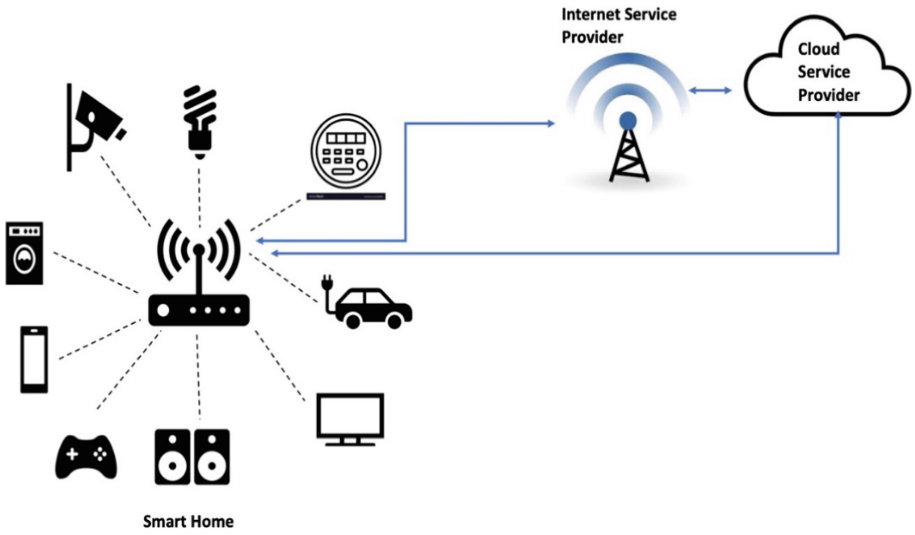

Fig. 1. Smart home router network

3.2 Future of Home Router Technology

The next generation of home routers may be able to provide enhanced connectivity through mobile networks, in addition to the fixed broadband connection, allowing the home router to tap into mobile networks when the fixed broadband does not provide adequate service.

In addition to the service network and guest network, the home router could have more channels opened up, with different security levels to facilitate the different services and numerous devices on the network (For example, a utility network, entertainment network, access network and so on). This will allow users and/or Service Providers to lockdown certain channels whilst relaxing the rule for some of the others.

3.3 The Role of Service Providers

In the UK, the ISPs mostly control the home router hardware the home user ends up within their home. The home user rarely has a say in the router hardware they are provided with. Security implications of this supply of home router hardware are that home users may end up with less secure and cheaper routers in their homes than the most secure and up-to-date technology available on the market. This is mostly because ISPs will provide hardware-based on what is most cost-effective and will give them better margins in what is a competitive market. The home user is rarely aware of the manufacturer of the hardware, 'the box', through which the ISP provide them broadband services.

The participants' general perception was that ISPs could do more than there were currently doing to make home routers more secure. However, the impact of low margins on home routers raises the question of whether ISPs have enough buying power and are in a good position to influence the design, functionality and features of home routers. The ISP has a relationship with the user and the manufacturer. The ISP is, therefore, key to the manufacturer understanding what the user really needs.

Cloud Service Providers

Some participants argued that Cloud Service Providers had better capability and are more equipped to protect home users from malware, virus and phishing attacks than ISPs. Cloud Service Providers like Amazon and Google have been able to harness a relationship with end-users in a way that traditional ISPs have not been able to do. They have managed to get end-users to become more accustomed to them and let them into their everyday lives – Google Home Assistant and Amazon Alexa and Echo, by offering the end-user what they want – a simple and easy lifestyle; thus, overcoming the main barrier that ISPs such as BT, Virgin, TalkTalk and Sky have had for a long time.

They have also demonstrated to the end-users that they can handle massive amounts of data securely. ISPs have not been able to get end-users to change their mindset about sharing their information freely with them.

3.4 The Role of Hardware and Hardware Manufacturers

Hardware manufacturers mostly focus on the design and production of hardware. They put primary hardware functionality ahead of security. This applies to both manufacturers of home routers and IoT devices. Security features may well slow down the performance of hardware, causing frustrations for end users. A gamer may be slowed down by the home router's security functionality, which may seek to block the gaming website or limit access, slowing down their performance.

Hardware manufacturers may contribute to the security of their devices by ensuring that their operating systems are from a secure, reputable source. Rather than go with the cheapest option all the time, they can carefully source and select their providers.

Most IoT devices usually seek to communicate with cloud endpoints and a few more sites and maybe other devices on the home network [10]. This was identified as a new threat to the home router network by one of the participants. They highlighted that manufacturers are gathering information about users and transferring them to the cloud without understanding how to protect that data. For example, a dishwasher manufacturer may not understand or know how to protect and manage the telemetry data their device collected about its user once that data is uploaded to the cloud.

Software

It was also highlighted that software, specifically, open-source software plays an important role in adding value to hardware. Most hardware manufacturers do not develop the software operating on their systems. Therefore, companies supplying this value-added software are also key stakeholders who must also provide home router security.

3.5 The Role of Citizen and Industry Groups

All the participants agreed that their levels of awareness were due to the fact that they are actively engaged and work within the security industry or citizen groups proactively doing work in the area. All the participants agreed that the general populations knowledge and awareness of security risks associated with their home router networks and devices were very limited and, in some cases, non-existent. The ratio in the general population is 80/20 rule.

There are several groups actively trying to raise user awareness around home router cyber security threats. These include Which, Smart Homes and Building Associations, Messaging Anti Abuse Working Group (MAAWG), Consumers International and IoTSF. Some groups will do specific targeted campaigns relevant to the specific groups that they support. It was highlighted that some of the bigger charities such as Victim Support, Citizens Advice and Neighbourhood Watch could help raise user awareness.

3.6 Cost of Providing Home Router Security

On average, businesses spend 4–10% of their IT budget on security. Whilst Service Providers may be spending huge amounts of money on protecting their own networks. There is no evidence to support the fact that Service Providers are spending anywhere near that amount on home router security. Security is being done on the cheap, but that needs to change as the future is online.

From a user's point of view, a home router may cost between £25 and £350 to buy. The cheaper ones are still quite basic, and the more expensive ones have inbuilt capabilities in their operating systems, offering better functionality and security.

The Covid 19 pandemic has seriously highlighted how important the Internet is to our everyday lives. With everything from education, healthcare, work, and social interactions being carried out remotely via the Internet's services. Accessibility to the Internet and technology has become even more critical than they were before. There are increasing concerns over a section of society who cannot afford to pay for the technology or service to benefit from using them. This adds an added layer of complication to the debate around who should pay for security.

3.7 Regulatory Role and Impact

Some participants argued that home router security should be considered a national issue as impacts of attacks due to IoT-enabled crime using home routers such as Distributed Denial of Service (DDoS) attacks are more likely to have major national infrastructure implications than for individuals. That makes it a more compelling issue for the government to get more involved to ensure that routers are secure.

All the participants agreed that regulations have and can play an important role in securing home routers and PITCHR. They also agreed that there is a clear lack of standards, frameworks and regulations in the IoT Space [11].

3.8 Who is/Should be Responsible for Home Router Security

Which of the home router network stakeholders is or should be responsible for home routers' security – the Service Provider, Hardware Manufacturer or the end-user?

Arguably, most end users are not in the best position to have the knowledge or technical know to decide how best to secure their network. Hardware manufacturers may have a role in determining the level of access that devices may need to function appropriately. They can help the end-user understand the right levels of settings users need to use with their devices by stipulating these in the user manuscripts of the devices. This could be difficult as hardware manufacturers may not necessarily know this information. They do not have a direct relationship with the end-user.

Therefore, most participants argued that the ISP is central to providing and ensuring home router security. If the trust levels between the end-user and the ISP are high, the ISP will warn the end-user of any potential threats and provide them with guidance on keeping themselves and their networks secure. The ISP could also forge an even closer relationship with the hardware manufacturer to understand how end-users use their hardware and the end-users' security issues.

3.9 User Awareness and Education

All participants agreed that one of the critical components to achieving home router security is user awareness.

They argued that most users are not aware of any issues associated with their IoT devices or home routers. As a result, they are not demanding that their Service Providers provide secure routers, nor are they factoring in security when purchasing IoT devices.

Most users are also unaware of IoT devices' complexity and connectivity to cloud services add to their home network. They may not be aware that devices are already communicating with each other in a way that requires little human intervention.

Privacy

Do users care about their privacy? Some participants shared the view that users only care about their privacy after they lose it. Users may lose money, financial details, personal details and/or may be victims of fraud and blackmail.

3.10 The Changing Nature of Home Router Cyber Security Landscape

Major aspects of understanding how the home router cyber security landscape is changing are to explore how the threats have evolved over the period of time (see Fig. 2); how they have influenced how technology has changed over the period of time; and, how security has kept up with the threats from criminal actors and whether or not those threats are driving and dictating the change in security. What is considered important to secure and what not to share with organisations and third parties, which could put the home user at risk.

Threats to the home network can be grouped into two: internal threats from inside the home and external threats from outside the home. IoT devices certainly change the nature of security threats from inside the home perimeter. In most cases, Service Providers may

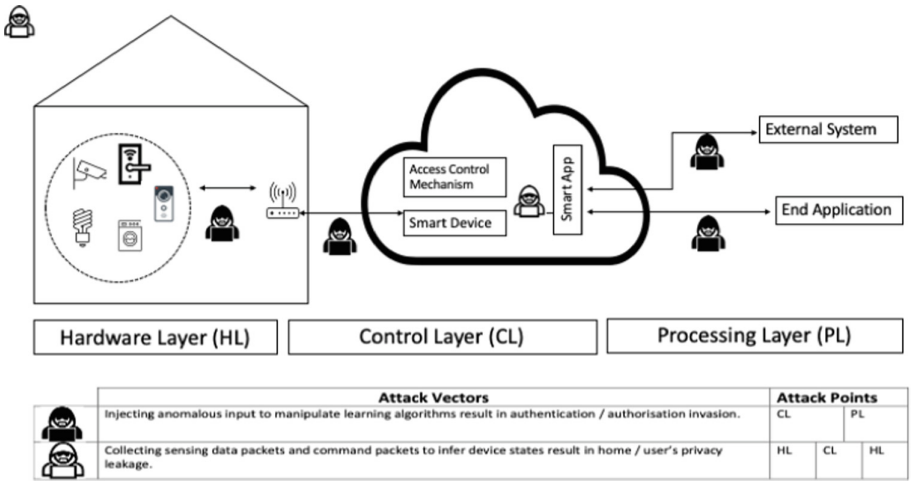

Fig. 2. Attack Vectors in the Home Network, adapted from Mao et al. [12]

be able to detect and manage external threats but not so easily or effectively internal threats that may be introduced by the end users themselves.

As machine to machine communication improves through ML, AI, and other technologies, chances of attacks similar to the Mirai botnets become increasingly likely. Criminals may also be able to use analytics from the home router network and associated IoT devices to inform their decisions on when to attack homes for example, the best time to burgle a home.

Most of the participants agreed that, ultimately, third party services might emerge, which may provide value-added services, in addition to what the service providers are already offering to make the home router network more secure.

4 Key Findings

The key findings of the study are presented as follows:

- The Prevention of IoT-enabled Crime using Home Routers requires a combined effort from all stakeholders.
- legislation – there are currently no specific regulations in the IoT space, although there may be discussions on-going in governments around the world.
- Stringent standards and frameworks are required for establishing baselines for home router security.
- There are no requirements on manufacturers to incorporate security into home routers and IoT devices by design and by default.
- Service Providers invest significantly into protecting their networks but the investment does not necessarily trickle down to the home router network, particularly inside the home environment.

- Service Providers do not collaborate sufficiently with each other, and sharing intelligence on threat landscape is limited, if at all. This makes it easy for cyber criminals to deploy the same techniques to several networks successfully.
- Automation of home router network security may be vital to the Prevention of IoT-enabled Crime using Home Routers.
- It is unclear who should be responsible for providing home router security.
- It is unclear who should pay for home router security
- the average end user of the home router does not have the knowledge and the capability to configure and secure their home router and devices.
- user awareness and education is vital in the Prevention of IoT-enabled Crime using Home Routers

All the combined stakeholder workshop participants agreed that the findings were an accurate representation of the focus group discussions.

5 Recommendations

The researchers would like to make the following recommendations based on the findings of the study:

1. Home router security must be available to all users by default and at an affordable cost.
2. ISPs must be responsible for ensuring that the routers they supply to home users have security capabilities that are enabled for the end-user.
3. ISPs must collaborate with Cloud Service Providers such as Microsoft, Amazon, and Google and other third-party providers to share intelligence on network traffic and device behaviours to effectively prevent IoT-enabled crime using home routers.
4. Service Providers must ensure that their service networks are secure to minimise security risks to connected devices.
5. It will be beneficial for IoT devices to be registered so that each device's activity on the network can be detected and traced to the device. This will help with the isolation of the device when malicious activities or traffic is detected from that behaviour.
6. Security on IoT devices must be improved by ensuring that manufacturers design and build devices with security by design and default.
7. Government must legislate for home router security and ensure that hardware manufacturers and Service Providers comply with security legislation.
8. Government must bring together all stakeholders to ensure that their perspectives inform its decisions.
9. Citizen groups could provide awareness to citizens about the threats of the home router network.
10. End users should be made aware of the nature of the risks associated with their home router network and the devices they use.

6 Conclusion

Smart homes are exponentially exposed to security vulnerabilities, with increasing numbers of smart devices being added to the home network. Most of the home network traffic into and out of the home is driven through the home router, which has minimal or no security built-in. Home router security is an afterthought, and none of the stakeholders, ISPs, hardware manufacturers, consumers, and government bodies is clearly responsible for implementing or enforcing home router security.

The absence of standards, frameworks and regulations in the IoT space and the lack of clarity around who is responsible for providing secure home defence systems continuous to cause significant challenges, exposing the home user to potential attacks, financial loss and loss of personal data.

It is anticipated that as users become more aware of the vulnerabilities and risks associated with their home router network, they may demand better security from their service providers and make informed choices when selecting providers or buying devices. They will implement basic security hygiene and best practice such as changing default passwords, regularly updating their device software, locking down devices and network where appropriate and proactively reporting suspected malicious activities on their network.

The cost of securing the home router environment should be spread out to make it more affordable to all end users. Service providers must be encouraged to dedicate part of their security budgets towards providing home router security and awareness training for the end-user.

Security of home routers must be by default and by design and automated wherever possible to reduce the burden on the end-user and improve the chances of securing the network without end-user intervention. Government regulations will play a critical part in ensuring that responsibility is placed in the Service Providers and hardware manufacturers' hands, not on the end-user who may not know or capability to secure their home network.

Acknowledgements. The study was funded by The Dawes Centre for Future Crime (DCFC) at UCL.

References

1. Ray, A.K., Bagwari, A.: IoT based smart home: security aspects and security architecture. In: IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), pp. 218–222 (2020)
2. Maple, C.: Security and privacy in the Internet of things. J. Cyber Policy **2**, 155–184 (2017)
3. Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., Lopez, J.: A survey of IoT-enabled cyberattacks: assessing attack paths to critical infrastructures and services. IEEE Commun. Surveys Tutorials **20**, 3453–3495 (2018)
4. Eurostat - Digital economy and society statistics - households and individuals https://ec.europa.eu/eurostat/databrowser/view/isoc_ci_in_h/default/bar?lang=en Accessed 5 Feb 2021
5. German Federal Office for Information Security: BSI TR-03148 Secure Broadband Router, BSI TR-03148:Secure Broadband Router (bund.de), Accessed Feb 2021

6. Teiss: All home routers sold by top European vendors feature security flaws https://www.teiss.co.uk/all-home-routers-vulnerable-threats/ Accessed 5 Feb 2021
7. Blythe, J., Sombatruang, N., Johnson, S.: What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? Journal of Cybersecurity **5**, 1–10 (2019)
8. Kebande, V.R., Karie, N.M., Michael, A., Malapane, S.M.G., Venter, H.S.: How an IoT-enabled "smart refrigerator" can play a clandestine role in perpetuating cyber-crime. In: IST-Africa Week Conference (IST-Africa), Windhoek, pp. 1–10 (2017)
9. Qorvo 'The WiFi Evolution', White Paper https://www.qorvo.com/-/media/files/qorvopublic/white-papers/qorvo-the-wi-fi-evolution-white-paper.pdf Accessed 30 Jan 2021
10. Mocrii, D., Chen, Y., Musilek, P.: 'IoT-based smart homes: a review of system architecture, software, communications, privacy and security. Internet of Things' **1**(2), 81–98 (2018)
11. Department for Digital, Culture, Media & Sports and National Cyber Security Centre https://www.gov.uk/government/news/government-to-strengthen-security-of-internet-connected-products#:~:text=These%20are%3A,on%20in%20a%20timely%20manner Accessed 20 Oct 2020
12. Mao, J., Lin, Q., Bia, J.: Application of learning algorithms in smart home IoT system security, Math. Found. Comput. 2–27 (2018)