ENHANCED SECURITY FRAMEWORK FOR THE SMART HOME AUTOMATION SYSTEM

Priyajot[1],Dr. Yogesh Kumar Sharma [2]

[1] Research Scholar Department of Computer science & Engineering; Shri JJT University Jhunjhunu Rajasthan

[2]Associate Professor & Research coordinator; Department of Computer science & Engineering; Shri JJT University Jhunjhunu Rajasthan

Abstract: Elderly care as well as enhance the quality of life for seniors, the users must be supplied with a lot of personal information about their homes and personal lives. This promising technology is being blocked by results in security and privacy. With the intent to empower end users, we did semi-struct interviews with 42 potential new and novice Smart Home customers. The issues they were concerned with focused on were connected around attacks on Smart Home data and devices, as well as the effect on users in general, to the importance of keeping their functionality balanced with the expectations of the people in their surroundings. In addition, we use measures from an interdisciplinary point of view to deal with the four topics The paper concludes with a few ideas for dealing with users' concerns, along with ideas for supporting application developers in crafting effective user-oriented digital assistants.

Keywords: Smart Home, Security, Privacy, Unauthorized access

Introduction

Smart Home technologies are thought to improve our everyday life, the functionality of our homes, and help the elderly to remain safe and independent. Thanks to SH (e.g., smart homes, lighting, communication, and sensors), household devices (e. e. g., washing machines, refrigerators) and the items they use (e. light bulbs, computers) and the things they consume are all inter-connected. It is possible to view, use, and control these integrated technologies to meet the needs of the SH user despite increased availability of SH technologies among end users, today's level of usage lags [4], [8] Possible causes include high cost, inflexibility, non-involvement, and impracticability for users security and privacy are yet another obstacle to adoption to put your technology to its full potential, you need information about your home and your private life This, however, can be abused by unscrupulous providers or third parties.

Concerns for personal privacy and security ranked high on people's technology acceptance needs among those with no SH, and older citizens' willingness to utilise health care solutions were prominent themes in focus groups on SH user requirements [8] and use patterns [13].

Though relatively little research has been done on analysing the security and privacy issues, the acceptance of virtual currency ownership has been inhibited by people who aren't yet comfortable with the advanced enough with SH technologies. This group, in particular, has a tremendous impact on decisions to implement SH technologies because of their concerns and perceptions.

This research intends to help people make good decisions on their own. In order to understand users' perceptions of our security and privacy SH technologies, we were required to conduct an extensive user investigation and answer all their concerns. We based our conclusions on our research and the recommendations on best practise from related disciplines, focusing on the users' concerns, and boosting transparency (see research procedure in Figure 1). We conclude from these findings that:

1. Dealing with potential and small groups of German semi-skilled users, we discovered four major issues that could be grouped into (1) threat to data and devices, (2) loss of control, (3) of functionality, and (4) risk of losing control on a global scale.
2. or in areas of in which psychological pressures can be exerted on SH residents, e.g.g.
3. In addition to comprehending the consumers' relative concern for security and functionality, this comparison sheds light on the problem.
4. It appears that user concern, coupled with technical security, is important but not sufficient in order to meet user needs. It is equally important to communicate privacy and security features to the customers. not only design actionable threat and danger notifications, but also ensure that customers have confidence in the overall security of the system Users might value transparency and automatic workflows because they want more control over end-user processes and support for manual processes.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

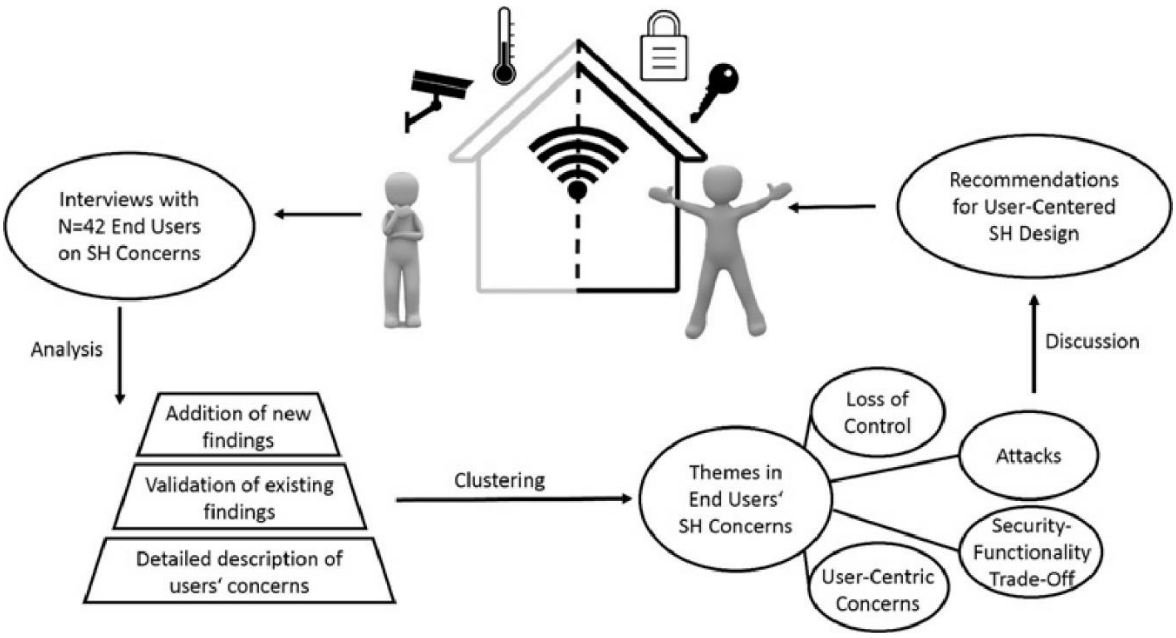
Interviews with
N=42 End Users
on SH Concerns
Analysis
Addition of new findings
Validation of existing findings
Detailed description of users' concerns
Clustering
Themes in End Users' SH Concerns
Loss of Control
Attacks
Security-Functionality Trade-Off
User-Centric Concerns
Discussion
Recommendations for User-Centered SH Design

Figure 1 Research Procedure and Contribution

.Literature review

Bitcoin and its underpinning technology i.e. blockhchain have been brought into the world after Satoshi Nakamoto published the popular paper in 2009[6]. Bitcoin was the most successful blockchain implementation to date. Blockchain is a peer-to-peer distributed blockchain system with communicating nodes to ensure safe and time-consuming documentation of transactions. Worden, Bullough and Haywood (2003) describe intelligent technology as one that is conscious of and capable of reacting to its surroundings. The authors explain further that several components are required for an intelligent technology in order to achieve these two attributes.

Even earlier Demiris (2004) research has found that the privacy and safety of patients must be covered in the use of telehealth technologies. The research concluded also that it could lead to improved quality, including home treatment of patients, by integrating smarter technology with facilities that can be used in the building. Reyhani and Mahdavi et al. (2007) claimed that, by supplying their username and password, first approved users must register on the verification system. The device approves the validity of the users during the second stage of the user verification. The system administrator receives training concepts from the user names and passwords for neural network training in the user registration level. Chan et al. (2009) also found that the increased advancement of technology and increased health costs saved money by offering intelligent assistance instead of a health facility. In order to predict arbitrary sensor events, Aipperspach et al. (2010) suggested an approach[2]. Their approach also has to do with sequence matching: sensor events are formed like Natural Language processing tools and words are used to construct a sensor data language model. In the most recent terms, this model will determine how likely a word is.

Robles et al. (2010) shows how successful our system is. The method consists of six strata. The approach consists of changing the network manager's sources, content filters, general email policies, network controls, and timely user-friendly solutions. Setting the source filters would reject incoming links before the Spam Mail is sent. The content filters review the mail content and block the unwanted emails that are sent in. It define a smart community as an ecosystem that consists of networked homes that use smart technology. The intelligent culture should also be considered virtual and restricted to a certain geographical area.

Das et al. (2012) suggest an algorithm to predict the user's next behaviour for the Smart Home Prediction (SHIP). In light of the latest commands from a user, the algorithm identifies and predicts the next command for matching sequences from the history gathered. There are no transient relationships between user behaviour. Recker (2013) also integrates the "who" and "where" use in well-defined issues of research in which who can be used in smart home technology firms and where the study was performed, namely China, can be carried out. Suresh, Daniel, Parthasarathy and Aswathy (2014) describe the Internet of Things as human, machine and connected things. According to the authors a smart object is a daily item or computer consisting of hardware components that can perform tasks, interact and be aware of the environment by using sensors and actuators that are required and are used in everyday life. Centered on the Ethereum Protocol, Griggs et al. (2014) implemented a private blockchain to allow safe and stable use of medical sensors, as well as eliminate safety hazards associated with remote patient monitoring. Their blockchain-based strategy will make it easier for practitioners to track their patients from distant sites on a safe, accessible and up-to-dated record, while providing secure, accurate and secure real-time monitoring.

Adrian's, A. A system for the monitoring and control of lighting, air temperatures, alarms, and other home appliances was designed et al

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

(2014). The solution to this project is to build an affordable Smart Home system with a view to reducing software costs and open source software by using shelf components without increasing complexity. However, the concept of healthcare, services, transportation, and other broad variety of applications has been more inclusive over the past decade. Although the concept of "things" has changed with the evolution of technology, the main objective is to make computer-sense knowledge without human interference. Ye et al. (2015) suggest the use of absolute temporal and related time information for the recognition of activities and indicate that temporal knowledge can considerably improve the accuracy of activity recognition.

Atzori (2015) notes that the fundamental paradigm is "potentially innumerable" applications. On the other hand, the P2P Foundation has a list of applications currently consisting of 33 applications using blockchain technology. Y. Sharma et al. (2015) suggested an invalid method to alert people about accidents that could happen in their home (such as people with visible and hearing impairments). The infrastructure uses sensor data and conducts incident detection analyses. These events are transmitted by smartphones to the residents.

McKeever et al. (2016) suggested the use of activity time for recognition [72] and the use of Dempster-principle Shafer's as an algorithm for learning. The findings of the evaluation indicate an increase of 70% of f-measure identification compared with a Naïve Bayes non-temporal classification. Both works are supervised, while our methods are unattended. Although Ledra Capital (2014), P2P Foundation (Soo, 2016) and the company Blockchain Technologies have been drawing up listings of future and existing applications, (2016) divide and broaden the applications into the four most frequently accepted categories, with subcategories establishing an organised list of applications.

Both Hui, Sherratt, and Sánchez (2016) announced that security problems are linked to all the technologies, so smart home technology must be equipped with more security measures. In particular, smart home technology allows for the interconnection of many devices. Airehrour, Gutierrez and Ray (2016) found that new or improved IoT system safety protocol and ID technology are required. Chen Shih-Chung et al. (2016) notes that the systems proposed by him can be easily adaptable for different applications such as machinery control in the machining, automobile, mobile wireless nodes navigation, automation, etc. Allen (2016) stresses that it is important to notice that Bitcoin-based blockchain technology is not sufficient to store currency details. Every type of information requiring an intermediary from third parties for authentication may potentially be stored in a blockchain such that it is autonomous (ibid).

In this sense, Mougayar (2016) builds on the points that Allen (2016) identifies and describes Blockchain more generally as "a network for value exchange," which retains the potential for decentralised store and transmission of information. A Home Indoor Positioning System (HIPS) proposed by Upadhyay et al. (2016) to position mobile devices such as smartphones and IoT locating applications. This paper includes an indoor device with Wi-Fi signals. A smart mobile robot creates radio maps for the proposed device automatically. In their document Shetel and Agarwal (2016) demonstrate that IoT allows Internet connectivity in real-time for all types of devices and physical objects. This system is virtualized and allows activities to be carried out without direct physical syncing between devices. With the support of smart devices and a high speed network, the IoT can do multiple jobs without reducing distances.

Lee et al. (2017), in her paper, demonstrate that the Internet of Thing website of physical objects includes the embedded technology that helps to create machines for contact between machines and people. This paper gives the autonomous system a complex data sheet on the parameters of the city climate. Chou et al. (2017) explains the remote controlled operation of a home automated device. This article addresses the installation issues, finds the different solutions across various network technologies and tries to maximise their use. The Home Automation System (HAS) requires a thorough analysis of the necessary HAS in a heterogeneous, eternal and distributive setting.

In their paper, Kamal et al. (2017) describes how Raspberry Pi was used as a network entrance. For sending and receiving the data, this paper uses the protocol MQTT (Message Queuing Telemetry Transport). The web page implementing the Access Control List (ACL) for the protection of data transactions is used to control all of the sensors used in this article. This article is linked with the Raspberry Pi and uses many sensors, both wired and wireless. Sahadevan et al. (2017) identify how the Internet of Things has a significant effect on customers and the electronics sector of businesses, which quickly operate in home automation, smart cities, automation industries, etc. Many power efficient and cost-effective sensors are available to developers on the market in order to create these applications. In the 2017 journal Financial Advances, Zhu and Zhou (2017) formulate blockchain characteristics for the study of blockchain applications on the Chinese stock crowdfunding market. In a survey conducted by Toschi, Campos and Cugnasca (2017) the home automation networks were compared and the typical market is heterogeneous. Users of intelligent home technology will buy goods from various suppliers, so that products cannot interact with each other. A study by Batista, Melício and Mendes (2017) suggested combining intelligent home and smart life with a paradigm of the Industry 4.0 Interconnected stuff which led to advantages such as connecting different technology solutions in the same architecture, enhanced security advantages, increased availability and faster recovery processes in case of failure.

Kshetri (2017) said China's IoT production is one of the most advanced in developing countries. In particular, several factors that have caused

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

the development to grow so rapidly in China. Argreaves and Hauxwell-Baldwin (2017) spoke about maintaining anonymity, confidentiality and safe storage for their customers through the applications offered by smart home technology companies. Recker (2017) also notes that research can be verified by current theory if there is an interest in testing phänomens. In this case, minimal theory has been established already in nature, and this study focuses in addition on understanding potential aspects due to the rapid growth of intelligent home technology.

Key Issues in Cyber Security and Privacy

It was once thought of as a useful tool for academics only, but has become essential for human survival, like electricity, water, food, and fuel. Everywhere there is money, there is also crime trying to take it from others or to keep it from them. the interconnected nature of the Internet means that cybersecurity is becoming increasingly important. Cybersecurity comprises three basic concepts: confidentiality, integrity, and availability.

- Security is about keeping data private. You can't achieve confidentiality with cryptography unless you manage to scramble the data so no one will know what you're saying or doing.
- Authorship is the verification that data is unaltered, and that the sender claims to have originated it. Non-repudiation is seen as a separate, but also part of authentication.
- Access allows for suitably authorised users to have unfettered access to data, communications infrastructure, and computer resources, and preventing unfit users from acquiring either one or both of these is the goal PriceWaterhouseCo conducts an annual survey on data security breaches every year. In 2015, 90% of large companies had been breached, up from 81% in 2014, and a double-digit growth rate of 14% for small businesses

Today, the Internet has become an essential component of business operations, making information security an essential requirement for all systems. On the other hand, however, as cybersecurity is further developed, so is cybercrime, as it becomes more sophisticated, more damaging, more comprehensive, and increasingly sophisticated. A very important element of security in Smart Homes is the use of trusted and accessible systems to support the use of network technologies. Security and privacy threats will outweigh the advantages of smart homes.

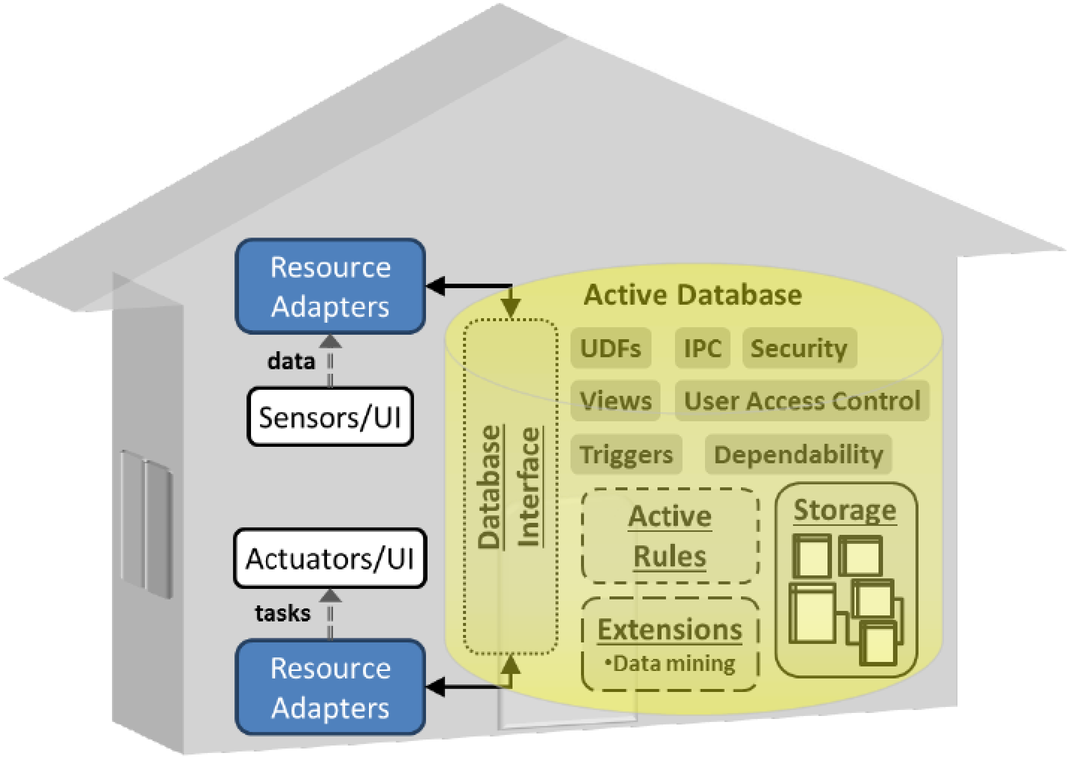

Figure 2: An overview of the integrated database-centric architecture.

Protecting your smart home from unauthorised access will allow you to run it even if you are away will allow you to use it even if you are away. However, while the Smart Home environment is a unique, threats do remain. Secrecy threats are those that compel the recipient to keep a secret regardless of whether they want to or not. It is an example of a compromise in home medical monitoring systems that can result in the unintentional disclosure of sensitive information. A great deal of seemingly insignificant data, such as the temperature of the home, could, when combined with the operating parameters of the air conditioner, give the alarm signal that someone is inside. Should loss

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

of confidentiality occur, the system is vulnerable to unauthorised access.

If there is authentication being attempted, either data is sensed or it is controlled. In addition, unauthenticated system alerts may lead a house controllers to believe that there is an emergency and allow a way out, when there is in fact, instead, they are actually helping to create it. Automatic updates will eventually be questioned. This will raise the question of whether or not they are trusted software updates.

There is a danger that consumers may become disinterested in your product or experience as a result of the access problems. Without sufficient administrative access, the entire system is vulnerable. It can be either unauthorised network connections or mismanagement of passwords. Even if you are unable to take control of the network, unauthorised connections may steal bandwidth or disrupt legitimate access. A wireless attack that floods the network with requests can depletes the energy may result in a Denial of Service (DoS).

It's a lot easier to clean your backyard than your office. If a system is network-wide accessible, it has a significant vulnerability. Attacks can be carried out via direct network connections or by compromising networked control systems are not only possible but also easy because of connected Smart Home systems. System independence is also applies. Even when the house is securely locked, the networks can be reached using wireless and power-line connectivity technologies.

Next on the list, you've got under-resourced system resources. Budgetary restraints have always placed an upper limit on the sophistication of security algorithms that could be implemented on device controllers, which have traditionally been small 8-bit microcontrollers with very limited computational and storage resources. System difference can be a weakness. Customers are provided with different technologies from vendors, as well as differing networking standards, in conjunction with software that may or may not be current. Since the devices are rarely documented, users often have to rely on printed or printed methods for information about their software, their operating systems, and security protocols.

Another common issue is bad or non-working firmware. The number of smart appliances that regularly patch security vulnerabilities is not many. People probably don't pay for security updates on devices that cost only a few dollars because they don't see much benefit. Standards adoption may be slower is a vulnerability. Despite having well-designed standards, most Smart Home devices fail to implement many, if any, measures of security. We believe the biggest threat to the absence of skilled Smart Home security staff capable of handling the complexities of a network. Few homeowners can afford regular network management assistance, regardless of their budget. Amateurs should be permitted to self-manage their systems instead of being expected to do it poorly, unsafely, and insecurely.

A Suitable Smart Home Architecture for Security

They've come up with different smart home architecture designs that each have their own problems. One of the most common design patterns is the middleware, as seen in cloud, gateway, and gateway architectures. In the following sections, the relevant security topics and implementation concerns are examined.

Many middleware systems and security products

Software that connects the middle-level hardware to the upper-level system. Over and above the lowest common denominator hardware specifications, the abstract interface and standard data exchange are used to promote simplicity. The middleware converts to device-specific accessors when it receives a request from a higher-layer request. when the application receives a response from the device, the middleware processes the necessary operations and formats and issues the commands to the lower level of functionality. Don't worry about the underlying details of the different hardware; the application only needs to make calls and perform provided middleware functions. Don't neglect the security and protection of the middleware - it should be considered at every level, from the hardware interaction to the more common interfaces.

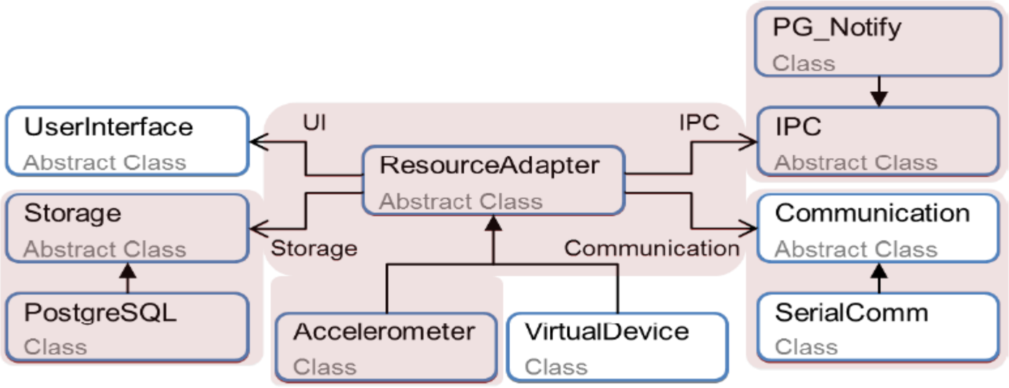

Figure 3: The class diagram describes the structure of a resource adapter

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Standard separation infrastructure, between open state-of-the-the-the-the-art message and separation of proprietary concerns. Conspicuous Communication (IC) Security Assertion Protection and Transport Layer Security (TLS) Secure Messaging and Media Protection (SMEP) is a middleware that addresses smart nodes communicating with each other. A device must join a group before it can communicate with others. Three security levels are available, but only two are occupied. There is no level 0 security. Multiparty cryptographic encryption is utilised under levels 1 and 2 for group authentication Under the other circumstances, it implements authentication at level 1 and uses encryption as a whole to safeguard data security.

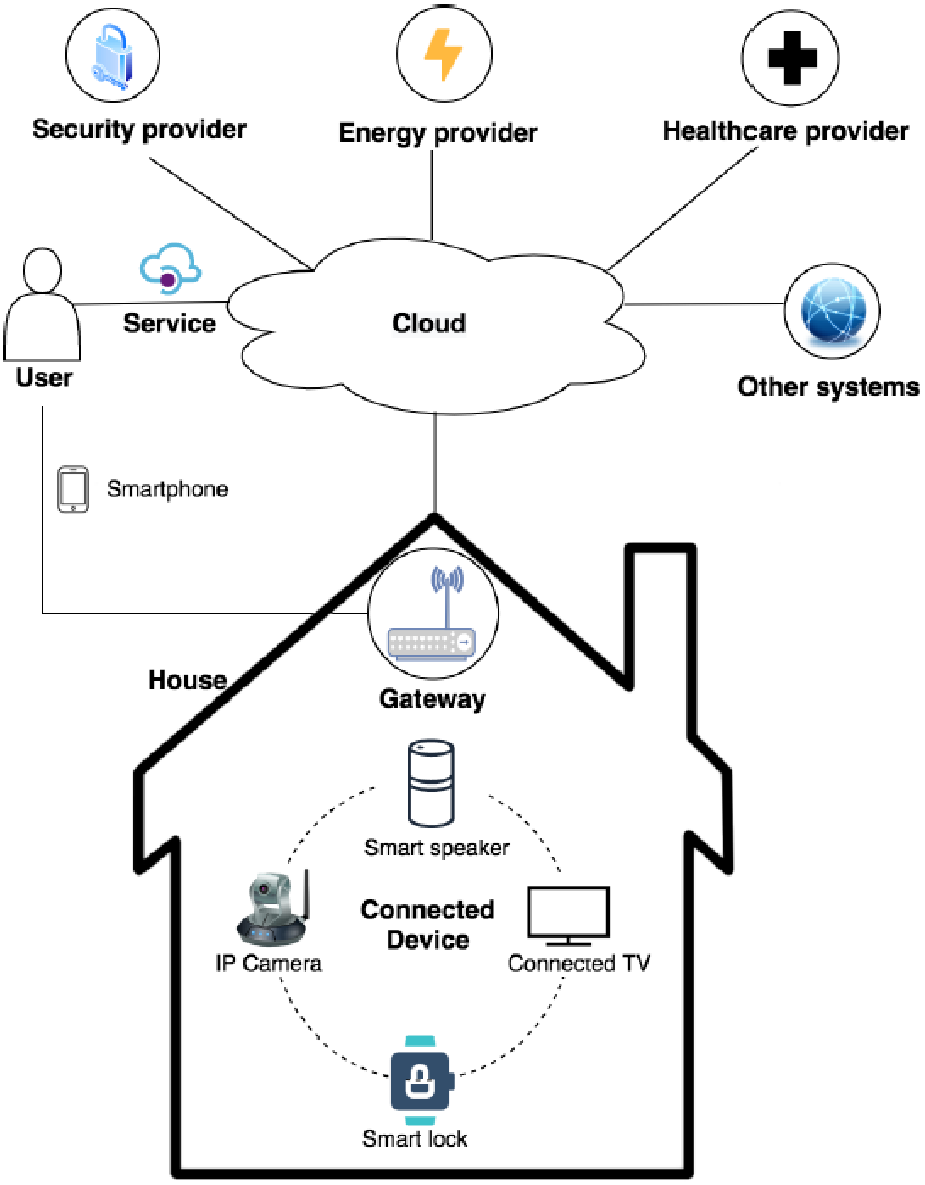

Fig. 4 Secured smart connected home architecture.

IoT middleware is being proposed for systems that currently have neither the memory nor the processing power in the host to support a complex heterogeneous network. Another concern for middleware bug threat: Middleware developers' programming issues could pose a security threat to IoT devices. thus we rule out the use of middleware for many Internet of Things applications

Security plays a key role in the decision of whether or not an IT infrastructure is cost-effective.

The interdependence of devices is an important to the Internet of Things. Such complex functions rely on high processing power, which few Internet of Things (IoT) devices have. Researchers have suggested cloud-based solutions to the problem of IoT device performance. For IoT devices, the cloud has the capability to monitor, collect, store, and process data. By analysing this data, the cloud can execute complex cloud-based IoT commands in response to user-defined policies. The IoT

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

architecture is described as the Cloud of Things in cloud-based terminology (CoT).

[The authors] recommend using the IETF's CoAP protocol for implementing an IoT cloud [23] There are three decoupled stages in the architecture. These are the network, protocol, and application logic. each stage includes an incoming event queue, a thread pool, which then queues new events, as well as its own logic, as well as an event handler that processes all of the stages. Lightweight DTLS is implemented for security and communication for this architecture.

According to a recent study, [33], the Home Area is well protected using cloud computing for network security. A home management system controls devices and manages policies, acting as the link between them and the access point. A team of researchers implemented H.M.M.S.S. functions in the cloud and the associated cloud service interactions are shown in the paper. This has been accomplished by means of applying end-to-end symmetric encryption to all the unique key assigned to each smart object in transit.

Cloud-based IoT empowers IoT with the ability to connect and interact locally; however, it replaces the use of local computation with a significant internet connectivity. On account of the constrained IoT devices, the amount of raw data available for them to handle is huge, which forces many of these devices to send a large amount of information to the cloud without pre-processing; thus, a high-speed, low-latency Internet connections are needed in remote and rural areas, but not always available.

Latency tends to increase when the servers are located overseas or when there is a lot of traffic. Any device connected to the network must have a broad attack surface and resources for full security protocols to be supported. Reduced connectivity may result in mission-critical systems, such as home healthcare and physical security systems being down. This is especially problematic since users lack control over their cloud services and therefore have to rely on them to implement appropriate and adequate security measures. We do not believe that cloud-based systems can provide a secure and available Smart Home on their own, so we don't believe they should be part of the Connected Home strategy.

A gateway structure is the portal to another part of the network.

IoT endpoints communicate with each other on the same network are resource-rich network processor network. Because it can be a critical for IoT device coordination as well, it is a primary management point for making inter- and intra-device connections as well. It can also serve as a link between the local Internet of Things (IoT) infrastructure and the cloud With a greater computing and storage capability, high-intensive tasks can be performed by the gateway instead of IoT devices. With regard to security, the gateway will safeguard user authentication and ensure that unauthorised or potentially dangerous data cannot be accessed. A firewall serves two functions: first, it protects the intelligent devices and their privacy from Internet attacks, and second, it restricts attack surface area.

Results & Analysis

Two themes emerged from this study. the first question was, the desirability of privacy among people working in the home sector, and the necessity of developing technology for those who use it The second issue, "choosing betweens the ethical dilemmas. You should be well aware of the fact that you will have to keep everything you know about this company's current employees private.

Notions of privacy are controversial, and therefore all people consider themselves free to make their views known. However, even though their social requirements are addressed, their limits remain unchanged. To illustrate privacy intrusions, here are three terms: data collection, storage, and eavesdropping; tracking, documenting, and photographing the personal activities of the subject; observation and photographing people as they move from place to place; peeping, esp of personal data; and the entry of people into private spaces; and eavesdropping, where one also documents the activity. "Privacy" questions were covered in the TV and radio interviews in Germany as well, but in addition, the opportunities for smart home technology were considered. Personally, privacy is a non-disruptive exchange of data, but it is said to be a fundamental right that must be respected.

Conclusion

This paper presents an application of edge-to-things computing which aims to offer a response to security threats within the Amst Homes. The presented solution focuses on locating the management system of the home IoT devices at the edge, so that the system may be controlled by the operator in the same way as current set-top-boxes are used for multimedia streaming. The network operator owns the smart home gateway, so it is in charge of security/privacy functionalities. The home automation network is, in our solution, isolated (higher layers) from the Internet, so all the communications are managed by the gateway. These communications are based on unified API, which presents the IoT devices functionalities independently from the device itself. For this, the network operator is in charge of updating constantly description of new vendors’ devices (and their unified API ontology) in the gateway, so new devices may be used and presented to the users through unified API. All these operations are performed through secure communication between the network operator’s management system and the smart home gateway.

The advantages of this solution for the network operator are related to the promotion of a new service (smart home) offered to the clients. This new service will have similar business plan as current multimedia streaming services such as VoD or IPTV. (These services are also offered by the network operator to the clients.)

The tests provided in this paper have confirmed that the implementation made from the scratch fulfills the specification. The tests have put special attention to security/privacy threats.

References

[1]. The Internet of things: Manage the complexity, seize the opportunity, white paper by Oracle, 2014. Available at: http://www.oracle.com/us/solutions/internetofthings/iot-managecomplexity-wp-2193756.pdf (Last checked: 2015-06-02).

[2]. S. Björnehaag, Test of a home energy management system at E.ON—an evalutaion of users's expectations and experience (Master thesis), Dept. of Energy Sciences, Lund University, 2012.

[3]. A. Fensel, V. Kumar, S.D.K. Tomic, End-user interfaces for energy-efficient semantically enabled smart homes, in: Energy Efficiency, Springer-Business Mediea, Dordrecht, 2014.

[4]. S. Radomirovic, Towards a model for security and privacy in the Internet of things, in: Proc. of the First Int'l Workshop on Security of the Internet of Things, 2010.

[5]. V. Rickebourg, D. Menga, The smart home concept: Our immediate future, in: 1st Int. Conf. on E-Learning in Industrial Electronics, 2006, pp. 23–28.

[6]. T. Denning, T. Kohno, H.M. Levy, Computer security and the modern home, Commun. ACM 56 (1) (2013) 94–103.

[7]. A.J. Bernheim Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, C. Dixon, Home automation in the wild: Challenges and opportunities, in: Proc. of the ACM Conference on Human Factors in Computing Systems, 2011.

[8]. T. Kowatsch, W. Maass, Critical privacy factors of Internet of things services: An empirical investigation with domain experts, in: Knowledge and Technologies in Innovative Information Systems, in: Lecture Notes in Business Information Processing, vol. 129, Springer, Dordrecht, 2012, pp. 200–211.

[9]. M. Rozenfeld, The value of privacy—Safeguarding your information in the age of the Internet of everything, The Institute, IEEE, March 7, 2014.

[10]. R. Weber, Accountability in the Internet of things, Comput. Law Secur. Rev. 27 (2011) 133–138.

[11]. T.R. Peltier, Information Security Risk Analysis, Auerbach Publications, Boca Raton, 2010.

[12]. Seth B., Dalal S., Kumar R. (2019) Hybrid Homomorphic Encryption Scheme for Secure Cloud Data Storage. In: Kumar R., Wiil U. (eds) Recent Advances in Computational Intelligence. Studies in Computational Intelligence, vol 823. Springer, Cham.

[13]. M. Weiss, A. Helfenstein, F. Mattern, T. Staake, Leveraging smart meter data to recognize home appliances, in: Proc. of the 10th IEEE Conf. on Pervasive Computing and Communication, 2012.

[14]. Armstrong, M. Krian, M. Jiang, A risk assessment framework and software toolkit for cloud service ecosystems, in: Proc. of the 2nd Int. Conf. on Cloud Computing, GRIDs, and Visualization, 2011.

[15]. T. Kirkham, D. Armstrong, K. Djermame, M. Jiang, Risk driven smart home resource management using cloud services, Future Gener. Comput. Syst. 38 (2013) 13–22.

[16]. S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, Proposed embedded security framework for Internet of things (IoT), in: Int. Conf. on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, 2011.

[17]. Seth B, Dalal S, Jaglan V, Le DN, Mohan S, Srivastava G Integrating encryption techniques for secure data storage in the cloud. Trans Emerg Telecommun Technol e4108, 1-24.

[18]. G. Gan, Z. Lu, J. Jiang, Internet of things security analysis, in: IEEE Conf. on Internet Technology and Applications, 2011.

[19]. R. van Kranenburg, E. Anzelmo, A. Bassi, D. Caprio, S. Dodson, M. Ratto, The Internet of things, in: Proc. of the First Berlin Symposium on Internet and Society, 2011.

[20]. C. Lee, L. Zappaterra, K. Choi, H.-A. Choi, Securing smart home: Technologies, security challenges, and security requirements, in: Proc. of the IEEE Conf. on Communications and Network Security, 2014.

[21]. S.R. Das, S. Chita, N. Peterson, B.A. Shirazi, M. Bhadkamkar, Home automation and security for mobile devices, in: Int. IEEE Conf. on Pervasive Communities and Service Clouds, 2011.

[22]. S. Notra, M. Siddiqi, H.H. Gharakheili, V. Sivaraman, R. Boreli, An experimental study of security and privacy risks with emerging household appliances, in: Proc. of Int. Workshop on Security and Privacy in Machine-to-Machine Communications, 2014.

[23]. A. Arabo, I. Brown, F. El-Moussa, Privacy in the age of mobility and smart devices in smart homes, in: Proc. of Int. Conf. on Social Computing, 2012.

[24]. D. Kozlov, J. Veijalainen, Y. Ali, Security and privacy threats in IoT architectures, in: Proc. of the 7th Int. Conf. on Body Area Networks, 2012.

[25]. C. Wuest, Smart security for today's smart homes: Don't let attackers spoil your christmas, Symantec media, European Union Agency for Network and Informat

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

ion Security, ENISA, 2014.

[26]. V. A. Sindekar, Y. K. Sharma, and D. Sharma, “A Guide for Selecting CMS Tools: Wordpress, Joomla, Drupal,” Studies in Indian Place Names, vol. 40, no. 35, pp. 621–626, 2020.

[27]. Baig, Hidayath Ali and Sharma, Dr. Yogesh Kumar and Ali, Syed Zakir, Privacy-Preserving in Big Data Analytics: State of the Art (September 12, 2020). International Conference on Business Management, Innovation & Sustainability (ICBMIS) 2020, Available at SSRN: https://ssrn.com/abstract=3713826 or http://dx.doi.org/10.2139/ssrn.3713826.

[28]. U. Eklund, C.M. Olsson, M. Ljungblad, Characterising software platforms from an architectural perspective, in: Software Architecture, Offical Blog. Available at: http://www.symantec.com/connect/blogs/smart-security-todays-smarthomes-dont-let-attackers-spoil-your-christmas (Last accessed: 2015-06-02).

[29]. D. Barnards-Wills, L. Marinos, S. Portesi, Threat landscape and good practice guide for smart home and converged in: Lecture Notes in Computer Science, vol. 7957, Springer, Berlin, 2013, pp. 344–347.

[30]. D.M. Han, J.H. Lim, Design and implementation of smart home energy management systems based on ZigBee, IEEE Trans. Consum. Electron. 56 (3) (2010) 1417–1425.

[31]. S.H. Yuang, ZigBee smart home automation systems, in: Wireless Sensor Networks: Principles, Design and Applications, Springer, London, 2014, pp. 263–274.

[32]. P. Baronti, P. Pillai, S. Chessa, A. Gotta, Y.F. Hu, Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards, Comput. Commun. 30 (7) (2007).

[33]. Ashok Kumar and Dr. Yogesh Kumar Sharma,” Reviewing cloud resource management schemes used in Cloud computing system”, International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 3 Issue 4, December 2016, pp. 104-111.

[34]. A. Hornsby, P. Belimpasakis, I. Defee, XMPP-based wireless sensor network and its integration into the extended home environment, in: IEEE 13th Int. Symp. on Consumer Electronics, 2009.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731