A Comparative Performance Study on Smart Home Automation and Security System Using Blockchain Technology

Priyajot[a], Dr. Yogesh Kumar Sharma[b]
[a]Research Scholar Department of Computer science & Engineering; Shri JJT University Jhunjhunu Rajasthan
[b]Associate Professor & Research coordinator; Department of Computer science & Engineering; Shri JJT University Jhunjhunu Rajasthan

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: Smart-home researchers' opinions and experiences suggest that privacy and choice are their main ethical concern. The researchers consider the private life of a person as a major problem when conducting research, though tending to see privacy in terms of information privacy, seldom see privacy as a personal privacy. In addition, we urge smart house-researchers to focus upon this. These are two major ethical issues. Is it necessary to concentrate on privacy? While some sort of privacy respect is a global social norm, it is fundamentally debated whether and when privacy is considered to be a moral principle coherently, as respect for privacy specifically limits the application of other moral requirements. Maybe due to the disputed moral significance, privacy-based moral arguments are at the forefront of many polarised bioethic discussions. Philosophical debates on privacy concentrate whether privacy is in the interests of one's own right (and therefore vulnerable to harm) or a cluster of other more fundamental interests, such as ownership and freedom interests.

Keywords: Smart Home, Security, Privacy, Unauthorized access

1. Background

In the near future, some 90 million people worldwide are projected to live in intelligent homes using technology to enhance home security, comfort and energy consumption [1]. A recent survey found more than a quarter in Sweden that they have a low level of awareness and control of energy use and 4/10 want to be more conscious of and regulated on energy use [12]. One way of providing householders with input, for example via a smart home automation system [3], about their energy usage. Studies have shown that energy consumption in households can be decreased by up to 20% in terms of receiving feedback [4].

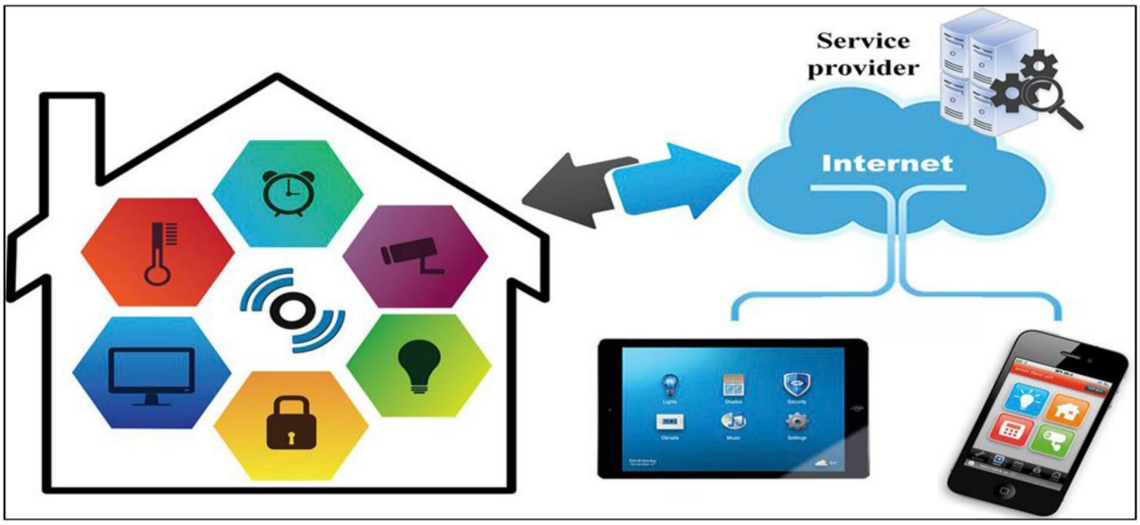

Fig. 1. Smart home architecture.

As such, intelligent home automation systems include popular devices which control the home's features, but not just enable and deactivate devices[5]. As a consequence of these technological developments, an intelligent home automation system can run devices independently and control the home on behalf of end users, i.e. people. Intelligent home automation has gained growing attention from industry players such as suppliers of energy and infrastructure as well as third parties providers of software and hardware [6,3]. There are different government agencies and communities as well as end-users among non-commercial stakeholders. Software and data-related information, resources, and infrastructures have started developed to address the challenges emerging from the complexities and heterogeneity of mass-connected services and devices, but no wave of existing practise at this stage is found for designing these smart systems [17]. For example, agreed alternative reference architecture or software frameworks, particularly so that they include system specifications otherwise critical such as security and privacy are currently missing [7,8]. [7,8]. As a result, there are many vertical solutions in which suppliers claim to help the entire chain with whatever unique software is necessary in the perspective of the individual business, from the sensors and equipment to the gates and servers. For example, this involves the introduction of additional services in addition to existing solutions with highly specialised APIs. This creates a dynamic situation in which consumer lock-in among many aspects is difficult to prevent, which can further compromise their engagement and dedication. It often causes challenges to incorporate system hygienic activities, such as risk analysis, privacy improvement and security compliance in these settings.

In addition, end users (such as tenants) may collect data on their buildings on aggregate energy usage (e.g., from the owners). Based on data collected, various services can be introduced, mainly by means of gamification methods, in order to increase energy awareness among end-users. In addition, an open mobile energy efficiency platform provides end-users with access to different applications through an online services and smartphone application ecosystem. It is also possible to link their services and applications to third party developers through an open API. In the research project. The risk understanding of consumers, partners, end-users' information use and possible abuse as well as the type of methods to incorporate safety enhancement measures into the design is not straightforward in IoT systems, particularly in those involving human actors, such as our SHAS and therefore requires considerable analysis[12]. In addition, measures must be developed to ensure the resilience of the IoT architecture to attacks, for example authentication, access protection and user privacy[10]. Indeed, one of the top obstacles to intelligent home automation was the complexity of achieving protection in IoT environments [27], which emphasises that this is a cumbersome but necessary task. In this paper, we use a standard risk analysis approach to determine system vulnerabilities and risks and their liking and possible impacts - i.e. risk exposure of the system. The SHAS risk analysis therefore builds on a well-known ISRA system, which is reported, for example, with Peltier [11]. A analysis of recent developments in science and industry is the basis of ISRA application for SHAS. It is important to examine not only device hazards relating to privacy and protection, but also the types of consumer privacy and home security scenarios involved in order to fully understand the effect of smart households. The principal contribution therefore are the findings of the risk evaluation on the smart home automation system, along with scenarios that demonstrate consumer privacy implications and a state-of-the-art analysis.

2. 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 (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 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.

3. Research Gaps

Need for security

This indicates that in examining and designing those aspects there were no methodological limits. Nevertheless, the relative transparency of the ISRA approach also points to the need for the complete incorporation of security into the design of smart homes with a more structural and aim-oriented approach [33].

User privacy condition

The threats to user privacy are a very critical area to explore in smart homes. While more and more parts of a house (and devices), all users and different stakeholders are linked to the Internet and not only to separate devices, access points can be obtained to the entire system, i.e. the home. This gives access to smart home knowledge not only to physical devices, but also to those devices and different stakeholders behind. When using a smart home device, digital tracks left (more or less voluntarily) may provide meta-information concerning family behaviours, i.e. help create broad, individual and collective profiles of the occupants of a house. Apart from its physical effects, e.g. in terms of burglaries, it can no longer be true that the house is a private domain. The house might instead become a public space in which the companies behind the linked equipment meet a single resident better than their closest friends or families [17].

Naturally, these kinds of outlooks are difficult to incorporate into a structural approach to risk analysis, but are important to define and clarify. To demonstrate this, we took into consideration private/public home scenarios, which may conclude that although the use of surveillance cameras seems remote it is necessary to include the risk of concept drift, the interconnection between system features and data, and increased use of various connected devices, some of which are user-intentional. Although the ISRA application to SHAS has not included these additions as points for evaluating the effect of the effects of the ISRA method, they are highly useful. It will therefore be important to discuss further the sensitivity, but also the threats and risk factors associated with the handling of personal information by the home environment and by the ecosystem of the individuals, engines, information and actors. An significant characteristic of this study is the added social actions of human actors (both as benevolent consumers and as villains). Another fascinating area to be discussed is strategy for managing user generated knowledge in smart homes. In addition, approaches to minimise sensitivity in information should also be included in the study, such as the flexible confidentiality of data and power. The home is no longer an enclosed private setting. More and more.

It would be advantageous if users themselves, e.g. as tenants, could customise the device according to their personal privacy choices conveniently and transparently rather than on a static boundary. A promising approach is good practises to direct end users in this process. Another important problem is how the information is processed, stored, managed and what rules, policies and standards govern the relation between device functions and data scenario.

4. Problem Formulation

There are some drawbacks to this study. This study, like research that uses the survey method, was likely to minimise measuring errors at the method stage. At the same time, this research is likely. In particular, the restriction refers in this research to the form of questionnaire used. Given the views, observations, and expectations of the subset of Jordanian people at a specified period, it is possible to deduce but not demonstrate the causality for consumers in intelligent homes in Jordan. This limits the statistical capacity to predict a broader range of conditions of market acceptance of intelligent homes.

However, as demonstrated by the strong validity and reliability of the analysis, the measurement errors were reduced and a potential study could be performed longitudinally, thereby allowing a greater degree of cause and effect. Furthermore, a qualitative approach may be used to examine evolving conditions and dimensions of acceptability or to get a deeper insight into any interconnectedness between variables. Second, this study focused on the characteristics of users at model level. But other considerations such as smart homes' characteristics and subjective expectations may be included and checked. Researchers are also encouraged to integrate the culture element in the future research model to better understand the views of consumers on smart homes technology.

5. Smart Home Automation and Security System Using Blockchain Technology

The architecture of a smart home application would contain the following entities: base station, sensor nodes, service agent, and a web application, as shown in Fig. 1.

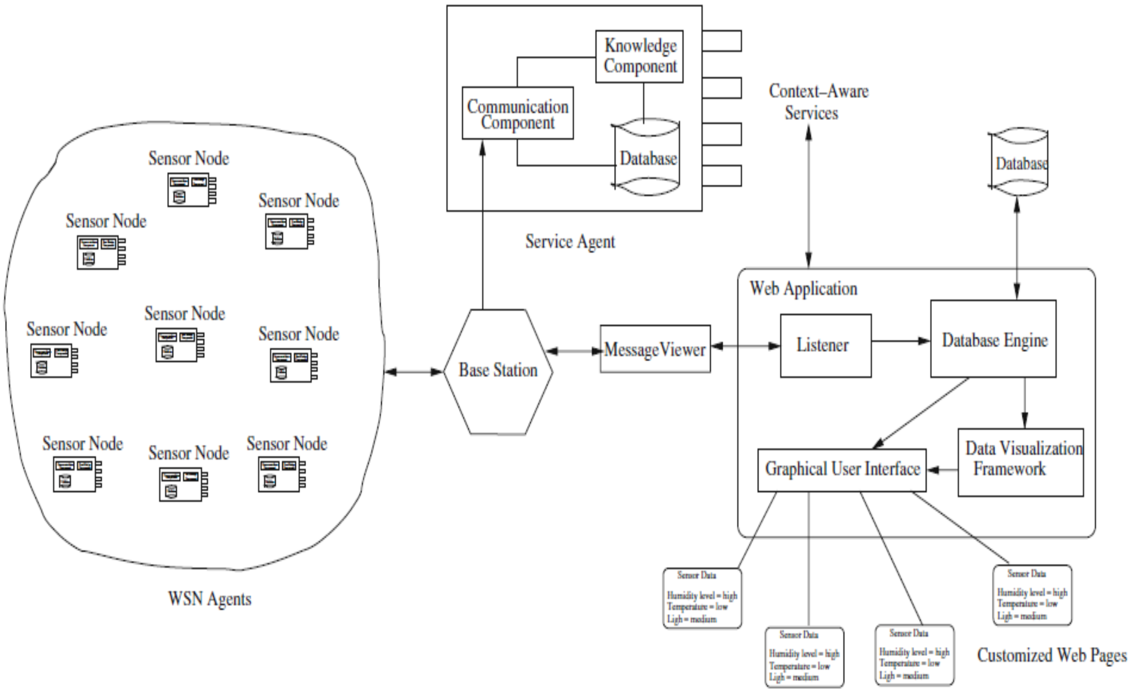

Fig. 2. Flow in Smart home

1. Base Station: A base station is a gateway to conventional and sensor networks (Internet).

2. Sensor nodes: the WSN for monitoring is generated by sensor nodes.

3. Service Agent: The service agent is responsible for collecting information from sensor data and nontrivial information. The service agent will have the following:

– Communication component: summarises application communication information

– Database: stores WSN data collected the portion of information: extracts data knowledge in a database

– Context-aware services for different applications: delivering personalised services. The service agent must be located at a computer or a gateway Node as it requires comprehensive compute and storage resources.

4. It offers custom web pages for end users. Web Application The following details:

– MessageViewer: read and send data from the base station through a TCP socket to the web application. – MessageViewer:

– Listener Component: A component that reads and makes the data accessible for the web application from MessageViewer.

– Database Engine: Speaking in connection databases like PostgreSQL are all sensor data.

– An engine of the backend database establishes a connection to the database and enforces safe queries. For example, for database engine, Hibernate2, Query can be applied to service/framework. Due to its simple running, no expense and support for larger tables, a PostgreSQL database is used. The Hibernate platform allows multiple user permissions, permissions and views.

– Graphical User Interface: A graphical front-end interface must be built to enable site access and display. The website, for example, offers an outline for the intelligent home, to be automatically modified with the introduction of new monitoring systems.

– Data Visualization Framework: graphs and layout for queries and sensor locations should be given on-the-fly for the application.

6. Results & Analysis

There are two topics that emerge from this research. The first was 'privacy' and included discussion of the desirability of personal privacy amongst smart-home project researchers, the need for and reasons of technology end-users' privacy. The second issue, "choice," centred on the contradiction between the resolution by end-users of ethical dilemms in research and the need for ethical decisions that restrict end-users' choices ultimately.

Confidentiality

Privacy is a "volatile and controversial concept" so that all rational objections are met. However, even though their limits are addressed, consistent social expectations preserve personal privacy. One taxonomy of privacy invasions included: data collection, storage and computers; distribution of information about persons; peeping, tracking, observing and photographing persons; intrusion or accessing "private" places; eavesdropping, wiretapping, reading letters; attention to persons; and forced disclosure of data.

In the interviews, German questions of privacy were also explored, encouraged to speculate on the challenges and possibilities of smart-home technology. Smart-home experts, in particular, describe privacy primarily as a non-interruptible data exchange rather than a personal invasion..

7. Conclusion

In support of this separation, it is possible that an individual is being monitored or tracked, while no information is being received or circulated, infringes their privacy. Apart from the metaphysical debates invited by this argument, those who do this work have strong practical consequences. Viewing researchers' conversations about privacy through the knowledge and physical secrecy lens provides insights into the difficulty of designing and supplying the public with home surveillance technology. In view of advanced technology such as encryption, protecting information privacy may seem to be a tractable problem.

In addition, the researchers had made significant efforts to decrease the possibility of unauthorised data sharing by isolation of internet networks, home servers and so on. While accidental data breaches are still possible, researchers were concerned with detecting and preventing these opportunities...

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. 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. 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 Information 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. 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.
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. 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.