ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Security Wireless IoT Protocol : In The Domain of Smart Homes

Dr. Archana Verma

Assistant Professor, Computer Science & Engineering , Bipin Tripathi Kumaon Institute of Technology, Dwarahat, Uttarakhand, India

ABSTRACT: While the application of IoT in smart technologies becomes more and more proliferated, the pandemonium of its protocols becomes increasingly confusing. More seriously, severe security deficiencies of these protocols become evident, as time-to-market is a key factor, which satisfaction comes at the price of a less thorough security design and testing. This applies especially to the smart home domain, where the consumer-driven market demands quick and cheap solutions. Here is an overview of IoT application domains and discusses the most important wireless IoT protocols for smart home, which are KNX-RF, EnOcean, Zigbee, Z-Wave and Thread. Finally, it describes the security features of said protocols and compares them with each other, giving advice on whose protocols are more suitable for a secure smart home.

KEYWORDS: IoT, smart technology, protocols, domain, homes, security, wireless, consumer

I.INTRODUCTION

Smart home systems achieved great popularity in the last decades as they increase the comfort and quality of life.[1] Most smart home systems are controlled by smartphones and microcontrollers. A smartphone application is used to control and monitor home functions using wireless communication techniques. We explore the concept of smart home with the integration of IoT services and cloud computing to it, by embedding intelligence into sensors and actuators, networking of smart things using the corresponding technology, facilitating interactions with smart things using cloud computing for easy access in different locations, increasing computation power, storage space and improving data exchange efficiency. In this chapter we present a composition of three components to build a robust approach of an advanced smart home concept and implementation.[2] The internet of things (IoT) paradigm refers to devices connected to the internet. Devices are objects such as sensors and actuators, equipped with a telecommunication interface, a processing unit, limited storage and software applications. It enables the integration of objects into the internet, establishing the interaction between people and devices among devices. The key technology of IoT includes radio frequency identification (RFID), sensor technology and intelligence technology. RFID is the foundation and networking core of the construction of IoT. Its processing and communication capabilities along with unique algorithms allows the integration of a variety of elements to operate as an integrated unit but at the same time allow easy addition and removal of components with minimum impact, making IoT robust but flexible to absorb changes in the environment and user preferences. To minimize bandwidth usage, it is using JSON, a lightweight version of XML, for inter components and external messaging[3]. Cloud computing is a shared pool of computing resources ready to provide a variety of computing services in different levels, from basic infrastructure to most sophisticated application services, easily allocated and released with minimal efforts or service provider interaction .In practice, it manages computing, storage, and communication resources that are shared by multiple users in a virtualized and isolated environment.[4] IoT and smart home can benefit from the wide resources and functionalities of cloud to compensate its limitation in storage, processing, communication, support in pick demand, backup and recovery. For example, cloud can support IoT service management and fulfillment and execute complementary applications using the data produced by it. Smart home can be condensed and focus just on the basic and critical functions and so minimize the local home resources

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

and rely on the cloud capabilities and resources. Smart home and IoT will focus on data collection, basic processing, and transmission to the cloud for further processing. To cope with security challenges, cloud may be private for highly secured data and public for the rest.[5]

IoT, smart home and cloud computing are not just a merge of technologies. But rather, a balance between local and central computing along with optimization of resources consumption. A computing task can be either executed on the IoT and smart home devices or outsourced to the cloud. Where to compute depends on the overhead tradeoffs, data availability, data dependency, amount of data transportation, communications dependency and security considerations. On the one hand, the triple computing model involving the cloud[6], IoT and smart home, should minimize the entire system cost, usually with more focus on reducing resource consumptions at home. On the other hand, an IoT and smart home computing service model, should improve IoT users to fulfill their demand when using cloud applications and address complex problems arising from the new IoT, smart home and cloud service model.Some examples of healthcare services provided by cloud and IoT integration[7]: properly managing information, sharing electronic healthcare records enable high-quality medical services, managing healthcare sensor data, makes mobile devices suited for health data delivery, security, privacy, and reliability, by enhancing medical data security and service availability and redundancy and assisted-living services in real-time, and cloud execution of multimedia-based health services.[8]

Smart home and IoT are rich with sensors, which generate massive data flows in the form of messages or events. Processing this data is above the capacity of a human being's capabilities . Hence, event processing systems have been developed and used to respond faster to classified events. In this section, we focus on rule management systems which can sense and evaluate events to respond to changes in values or interrupts. The user can define event-triggered rule and to control the proper delivery of services.[9] A rule is composed of event conditions, event pattern and correlation-related information which can be combined for modeling complex situations. It was implemented in a typical smart home and proved its suitability for a service-oriented system.The system can process large amounts of events, execute functions to monitor, navigate and optimize processes in real-time. It discovers and analyzes anomalies or exceptions and creates reactive/proactive responses, such as warnings and preventing damage actions. Situations are modeled by a user-friendly modeling interface for event-triggered rules.[10] When required, it breaks them down into simple, understandable elements. The proposed model can be seamlessly integrated into the distributed and service-oriented event processing platform.The evaluation process is triggered by events delivering the most recent state and information from the relevant environment. The outcome is a decision graph representing the rule. It can break down complex situations to simple conditions, and combine them with each other, composing complex conditions. The output is a response event raised when a rule fires. The fired events may be used as input for other rules for further evaluation. Event patterns are discovered when multiple events occur and match a pre-defined pattern.[11] Due to the graphical model and modular approach for constructing rules, rules can be easily adapted to domain changes. New event conditions or event patterns can be added or removed from the rule model. Rules are executed by event services, which supply the rule engine with events and process the evaluation result. To ensure the availability of suitable processing resources, the system can run in a distributed mode, on multiple machines and facilitate the integration with external systems, as well. The definition of relationships and dependencies among events that are relevant for the rule processing, are performed using sequence sets, generated by the rule engine. The rule engine constructs sequences of events relevant to a specific rule condition to allow associating events by their context data. Rules automatically perform actions in response when stated conditions hold. Actions generate response events, which trigger response activities. Event patterns can match temporal event sequences, allowing the description of home situations where the occurrences of events are relevant. For example, when the door is kept open too long.[12]

The following challenges are known with this model: structure for the processed events and data, configuration of services and adapters for processing steps, including their input and output parameters, interfaces to external systems for sensing data and for responding by executing transactions, structure for the processed events and data, data transformations, data analysis

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

and persistence. It allows to model which events should be processed by the rule service and how the response events should be forwarded to other event services. The process is simple: data is collected and received from adapters which forward events to event services that consume them. Initially the events are enriched to prepare the event data for the rule processing. For example, the response events are sent to a service for sending notifications to a call agent, or to services which transmit event delay notifications and event updates back to the event management system.[13]

II.DISCUSSION

To demonstrate the benefits of the advanced smart home, we use RSA, a robust asymmetric cryptography algorithm, which generates a public and private key and encrypts/decrypts messages. Using the public key, everyone can encrypt a message, but only these who hold the private key can decrypt the sent message. Generating the keys and encrypting/decrypting messages, involves extensive calculations, which require considerable memory space and processing power. Therefore, it is usually processed on powerful computers built to cope with the required resources. However, due to its limited resources, running RSA in an IoT device is almost impossible, and so, it opens a security gap in the Internet, where attackers may easily utilize. To cope with it, we combine the power of the local smart home processors to compute some RSA calculations and forward more complicated computing tasks to be processed in the cloud. The results will then be transferred back to the IoT sensor to be compiled and assembled together, to generate the RSA encryption/decryption code, and so close the mentioned IoT security gap.[14] This example demonstrates the data flow among the advanced smart home components. Where, each component performs its own stack of operations to generate its unique output. However, in case of complicated and long tasks it will split the task to sub tasks to be executed by more powerful components. Referring to the RSA example, the IoT device initiates the need to generate an encryption key and so, sends a request message to the RSA application, running in the smart home computer. The smart home computer then asks the "prime numbers generation" application running on cloud, to provide p and q prime numbers. Once p and q are accepted, the encryption code is generated. In a later stage, an IoT device issues a request to the smart home computer to encrypt a message, using the recent generated RSA encryption key. [15] The encrypted message is then transferred back to the IoT device for further execution. A similar scenario may be in the opposite direction, when an IoT device gets a message it may request the smart home to decrypt it.[16]

To summarize, the RSA scenarios depict the utilization of the strength of the cloud computing power, the smart home secured computing capabilities and at the end the limited power of the IoT device. It proves that without this automatic cooperation, RSA would not be able to be executed at the IoT level.

A more practical example is where several detached appliances, such as an oven, a slow cooker and a pan on the gas stove top, are active in fulfilling the resident request. The resident is getting an urgent phone call and leaves home immediately, without shutting off the active appliances. In case the relevant IoTs have been tuned to automatically shut down based on a predefined rule, it will be taken care at the IoT level. Otherwise, the smart home realizes the resident has left home [the home door has been opened and then locked, the garage has been opened, the resident's car left, the main gate was opened and then closed, no one was at home] and will shut down all active devices classified as risk in case of absence. It will send an appropriate message to the mailing list defined for such an occasion.[17]

The smart home application updates the home database in the cloud to allow remote people access it and get the latest status of the home. A typical IoT platform contains: device security and authentication, message brokers and message queuing, device administration, protocols, data collection, visualization, analysis capabilities, integration with other web services, scalability, APIs for real-time information flow and open source libraries. IoT sensors for home automation are known by their sensing capabilities, such as: temperature, lux, water level, air composition, surveillance video cameras, voice/sound, pressure, humidity, accelerometers, infrared, vibrations and ultrasonic. Some of the most commonly used smart home sensors

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

are temperature sensors, most are digital sensors, but some are analog and can be extremely accurate. Lux sensors measure the luminosity. Water level ultrasonic sensors.[18]

Float level sensors offer a more precise measurement capability to IoT developers. Air composition sensors are used by developers to measure specific components in the air: CO monitoring, hydrogen gas levels measuring, nitrogen oxide measure, hazardous gas levels. Most of them have a heating time, which means that it requires a certain time before presenting accurate values. It relies on detecting gas components on a surface only after the surface is heated enough, values start to show up. Video cameras for surveillance and analytics. A range of cameras, with a high-speed connection. Using Raspberry Pi processor is recommended as its camera module is very efficient due to its flex connector, connected directly to the board.

Sound detectors are widely used for monitoring purposes, detecting sounds and acting accordingly. Some can even detect ultra-low levels of noise, and fine tune among various noise levels.[19]

Humidity sensors sense the humidity levels in the air for smart homes. Its accuracy and precision depend on the sensor design and placement. Certain sensors like the DHT22, built for rapid prototyping, will always perform poorly when compared to high-quality sensors like HIH6100. For open spaces, the distribution around the sensor is expected to be uniform requiring fewer corrective actions for the right calibration.

Smart home communication protocols: bluetooth, Wi-Fi, or GSM. Bluetooth smart or low energy wireless protocols with mesh capabilities and data encryption algorithms. Zigbee is mesh networked, low power radio frequency-based protocol for IoT. X10 protocol that utilizes powerline wiring for signaling and control. Insteon, wireless and wireline communication. Z-wave specializes in secured home automation. UPB, uses existing power lines. Thread, a royalty-free protocol for smart home automation. ANT, an ultra-low-power protocol for building low-powered sensors with a mesh distribution capability. The preferred protocols are bluetooth low energy, Z-wave, Zigbee, and thread. Considerations for incorporating a gateway may include: cloud connectivity, supported protocols, customization complexity and prototyping support. Home control is composed of the following: state machine, event bus, service log and timer.[20]

Modularity: enables the bundle concept, runtime dynamics, software components can be managed at runtime, service orientation, manage dependencies among bundles, life cycle layer: controls the life cycle of the bundles, service layers: defines a dynamic model of communication between various modules, actual services: this is the application layer. Security layer: optional, leverages Java 2 security architecture and manages permissions from different modules.OpenHAB is a framework, combining home automation and IoT gateway for smart homes. Its features: rules engine, logging mechanism and UI abstraction. Automation rules that focus on time, mood, or ambiance, easy configuration, common supported hardware:Domoticz architecture: very few people know about the architecture of Domoticz, making it extremely difficult to build applications on it without taking unnecessary risks in building the product itself. For example, the entire design of general architecture feels a little weird when you look at the concept of a sensor to control to an actuator. Building advanced applications with Domoticz can be done using OO based languages.[21]

Deployment of blockchain into home networks can easily be done with Raspberry Pi. A blockchain secured layer between devices and gateways can be implemented without a massive revamp of the existing code base. Blockchain is a technology that will play a role in the future to reassure them with revolutionary and new business models like dynamic renting for Airbnb.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

III.RESULTS

Home automation or domotics is building automation for a home, called a smart home or smart house. A home automation system will monitor and/or control home attributes such as lighting, climate, entertainment systems, and appliances. It may also include home security such as access control and alarm systems. When connected with the Internet, home devices are an important constituent of the Internet of Things ("IoT").A home automation system typically connects controlled devices to a central smart home hub (sometimes called a "gateway"). The user interface for control of the system uses either wall-mounted terminals, tablet or desktop computers, a mobile phone application, or a Web interface that may also be accessible off-site through the Internet.While there are many competing vendors, there are increasing efforts towards open source systems. However, there are issues with the current state of home automation including a lack of standardized security measures and deprecation of older devices without backwards compatibility.Home automation has high potential for sharing data between family members or trusted individuals for personal security and could lead to energy saving measures with a positive environmental impact in the future.[22]

Home automation is prevalent in a variety of different realms, including:

- Heating, ventilation and air conditioning (HVAC): it is possible to have remote control of all home energy monitors over the internet incorporating a simple and friendly user interface.
- Lighting control system: a "smart" network that incorporates communication between various lighting system inputs and outputs, using one or more central computing devices.
- Occupancy-aware control system: it is possible to sense the occupancy of the home using smart meters and environmental sensors like CO_2 sensors, which can be integrated into the building automation system to trigger automatic responses for energy efficiency and building comfort applications.
- Appliance control and integration with the smart grid and a smart meter, taking advantage, for instance, of high solar panel output in the middle of the day to run washing machines.[23]
- Home robots and security: a household security system integrated with a home automation system can provide additional services such as remote surveillance of security cameras over the Internet, or access control and central locking of all perimeter doors and windows.[24]
- Leak detection, smoke and CO detectors
- Laundry-folding machine, self-making bed
- Indoor positioning systems (IPS).
- Home automation for the elderly and disabled.
- Pet and baby care, for example tracking the pets and babies' movements and controlling pet access rights.
- Air quality control (inside and outside). For example, Air Quality Egg is used by people at home to monitor the air quality and pollution level in the city and create a map of the pollution.
- Smart kitchen, with refrigerator inventory, premade cooking programs, cooking surveillance, etc.
- Voice control devices like Amazon Alexa or Google Home used to control home appliances or systems.[16]

Utilizing home automation could lead to more efficient and intelligent energy-saving techniques. By integrating information and communication technologies (ICT) with renewable energy systems such as solar power or wind power, homes can autonomously make decisions about whether to store energy or expend it for a given appliance, leading to overall positive environmental impacts and lower electricity bills for the consumers using the system. To do this, researchers propose using

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

data from sensors regarding consumer activity within the home to anticipate consumer needs and balance that with energy consumption.

Furthermore, home automation has a large potential regarding family safety and security. According to a 2015 survey done by iControl, the primary drivers of the demand for smart and connected devices are first "personal and family security", and second "excitement about energy savings". Home automation includes a variety of smart security systems and surveillance setups. This allows consumers to monitor their homes while away, and to give trusted family members access to that information in case anything bad happens.[18]

The Internet of things (IoT) describes physical objects (or groups of such objects) with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks.[1][2][3][4][5] Internet of things has been considered a misnomer because devices do not need to be connected to the public internet, they only need to be connected to a network,[6] and be individually addressable.[7][8]

The field has evolved due to the convergence of multiple technologies, including ubiquitous computing, commodity sensors, increasingly powerful embedded systems, as well as machine learning.[9] Traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), independently and collectively enable the Internet of things.[10] In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "smart home", including devices and appliances (such as lighting fixtures, thermostats, home security systems, cameras, and other home appliances) that support one or more common ecosystems, and can be controlled via devices associated with that ecosystem, such as smartphones and smart speakers. IoT is also used in healthcare systems.[11]

There are a number of concerns about the risks in the growth of IoT technologies and products, especially in the areas of privacy and security, and consequently, industry and governmental moves to address these concerns have begun, including the development of international and local standards, guidelines, and regulatory frameworks.[12]

The extensive set of applications for IoT devices[12] is often divided into consumer, commercial, industrial, and infrastructure spaces.

Consumers

A growing portion of IoT devices is created for consumer use, including connected vehicles, home automation, wearable technology, connected health, and appliances with remote monitoring capabilities.

Home automation

IoT devices are a part of the larger concept of home automation, which can include lighting, heating and air conditioning, media and security systems and camera systems.Long-term benefits could include energy savings by automatically ensuring lights and electronics are turned off or by making the residents in the home aware of usage.[15]

A smart home or automated home could be based on a platform or hubs that control smart devices and appliances. For instance, using Apple's HomeKit, manufacturers can have their home products and accessories controlled by an application in iOS devices such as the iPhone and the Apple Watch. This could be a dedicated app or iOS native applications such as Siri. This can be demonstrated in the case of Lenovo's Smart Home Essentials, which is a line of smart home devices that are controlled through Apple's Home app or Siri without the need for a Wi-Fi bridge. There are also dedicated smart home hubs that are offered as standalone platforms to connect different smart home products and these include the Amazon Echo, Google Home, Apple's HomePod, and Samsung's SmartThings Hub. In addition to the commercial systems, there are many non-proprietary, open source ecosystems; including Home Assistant, OpenHAB and Domoticz. [13]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Elder care

One key application of a smart home is to provide assistance to elderly individuals and to those with disabilities. These home systems use assistive technology to accommodate an owner's specific disabilities. Voice control can assist users with sight and mobility limitations while alert systems can be connected directly to cochlear implants worn by hearing-impaired users. They can also be equipped with additional safety features, including sensors that monitor for medical emergencies such as falls or seizures. Smart home technology applied in this way can provide users with more freedom and a higher quality of life.

The term "Enterprise IoT" refers to devices used in business and corporate settings. By 2014, it is estimated that the EIoT will account for 9.1 billion devices.[14]

Organizations

Medical and healthcare

The Internet of Medical Things (IoMT) is an application of the IoT for medical and health-related purposes, data collection and analysis for research, and monitoring. The IoMT has been referenced as "Smart Healthcare"[as the technology for creating a digitized healthcare system, connecting available medical resources and healthcare services.[17]

IoT devices can be used to enable remote health monitoring and emergency notification systems. These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants, such as pacemakers, Fitbit electronic wristbands, or advanced hearing aids. Some hospitals have begun implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up. It can also adjust itself to ensure appropriate pressure and support are applied to the patient without the manual interaction of nurses. A 2015 Goldman Sachs report indicated that healthcare IoT devices "can save the United States more than $300 billion in annual healthcare expenditures by increasing revenue and decreasing cost. Moreover, the use of mobile devices to support medical follow-up led to the creation of 'm-health', used analyzed health statistics." [11]

Specialized sensors can also be equipped within living spaces to monitor the health and general well-being of senior citizens, while also ensuring that proper treatment is being administered and assisting people to regain lost mobility via therapy as well. These sensors create a network of intelligent sensors that are able to collect, process, transfer, and analyze valuable information in different environments, such as connecting in-home monitoring devices to hospital-based systems. Other consumer devices to encourage healthy living, such as connected scales or wearable heart monitors, are also a possibility with the IoT. End-to-end health monitoring IoT platforms are also available for antenatal and chronic patients, helping one manage health vitals and recurring medication requirements.[24]

Advances in plastic and fabric electronics fabrication methods have enabled ultra-low cost, use-and-throw IoMT sensors. These sensors, along with the required RFID electronics, can be fabricated on paper or e-textiles for wireless powered disposable sensing devices. Applications have been established for point-of-care medical diagnostics, where portability and low system-complexity is essential.As of 2015 IoMT was not only being applied in the clinical laboratory industry, but also in the healthcare and health insurance industries. IoMT in the healthcare industry is now permitting doctors, patients, and others, such as guardians of patients, nurses, families, and similar, to be part of a system, where patient records are saved in a database, allowing doctors and the rest of the medical staff to have access to patient information Moreover, IoT-based systems are patient-centered, which involves being flexible to the patient's medical conditions. IoMT in the insurance industry provides access to better and new types of dynamic information. This includes sensor-based solutions such as biosensors, wearables, connected health devices, and mobile apps to track customer behavior. This can lead to more accurate underwriting and new pricing models. [21]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

The application of the IoT in healthcare plays a fundamental role in managing chronic diseases and in disease prevention and control. Remote monitoring is made possible through the connection of powerful wireless solutions. The connectivity enables health practitioners to capture patient's data and apply complex algorithms in health data analysis.[20]

IV.CONCLUSIONS

Even though scientists, engineers, and managers across the world are continuously working to create and exploit the benefits of IoT products, there are some flaws in the governance, management and implementation of such projects. Despite tremendous forward momentum in the field of information and other underlying technologies, IoT still remains a complex area and the problem of how IoT projects are managed still needs to be addressed. IoT projects must be run differently than simple and traditional IT, manufacturing or construction projects. Because IoT projects have longer project timelines, a lack of skilled resources and several security/legal issues, there is a need for new and specifically designed project processes. The following management techniques should improve the success rate of IoT projects:

- A separate research and development phase
- A Proof-of-Concept/Prototype before the actual project begins
- Project managers with interdisciplinary technical knowledge
- Universally defined business and technical jargon[23]

REFERENCES

1. Gillis, Alexander (2014). "What is internet of things (IoT)?". IOT Agenda. Retrieved 17 August 2014.
2. ^ Brown, Eric (20 September 2016). "21 Open Source Projects for IoT". Linux.com. Retrieved 23 October 2016.
3. ^ "Internet of Things Global Standards Initiative". ITU. Retrieved 26 June 2015.
4. ^ Hendricks, Drew. "The Trouble with the Internet of Things". London Datastore. Greater London Authority. Retrieved 10 August 2015.
5. ^ Shafiq, Muhammad; Gu, Zhaoquan; Cheikhrouhou, Omar; Alhakami, Wajdi; Hamam, Habib (3 August 2015). "The Rise of "Internet of Things": Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks". Wireless Communications and Mobile Computing. 2015: e8669348. doi:10.1155/2015/8669348. ISSN 1530-8669.
6. ^ Beal, Vangie (1 September 1996). "What is a Network?". Webopedia. Retrieved 22 November 2015.
7. ^ Internet of things and big data analytics toward next-generation intelligence. Nilanjan Dey, Aboul Ella Hassanien, Chintan Bhatt, Amira Ashour, Suresh Chandra Satapathy. Cham, Switzerland. 2015. p. 440. ISBN 978-3-319-60435-0. OCLC 1001327784.
8. ^ "Forecast: The Internet of Things, Worldwide, 2013". Gartner. Retrieved 3 March 2015.
9. ^ Hu, J.; Niu, H.; Carrasco, J.; Lennox, B.; Arvin, F., "Fault-tolerant cooperative navigation of networked UAV swarms for forest fire monitoring" Aerospace Science and Technology, 2015.
10. ^ Hu, J.; Lennox, B.; Arvin, F., "Robust formation control for networked robotic systems using Negative Imaginary dynamics" Automatica, 2015.
11. ^ Laplante, Phillip A.; Kassab, Mohamad; Laplante, Nancy L.; Voas, Jeffrey M. (2015). "Building Caring Healthcare Systems in the Internet of Things". IEEE Systems Journal. 12 (3): 3030–3037. Bibcode:2015ISysJ..12.3030L. doi:10.1109/JSYST.2016.2662602. ISSN 1932-8184. PMC 6506834. PMID 31080541.
12. ^ "The New York City Internet of Things Strategy". www1.nyc.gov. Retrieved 6 September 2014.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

13. Hill, Jim (12 September 2015). "The smart home: a glossary guide for the perplexed". T3. Retrieved 27 March 2016.
14. ^ Home Automation & Wiring (1 ed.). New York: McGraw-Hill/TAB Electronics. 1999-03-31. ISBN 978-0-07-024674-4.
15. ^ Rye, Dave (October 1999). "My Life at X10". AV and Automation Industry eMagazine. AV and Automation Industry eMagazine. Archived from the original on September 30, 2014. Retrieved October 8, 2014.
16. ^ "1.5 Million Home Automation Systems Installed in the US This Year". ABI Research. November 19, 2012. Retrieved 2016-11-22.
17. ^ "Smart Home - United States | Statista Market Forecast". Statista. Retrieved 2014-11-07.
18. ^ Caccavale, Michael (September 24, 2015). "The Impact Of The Digital Revolution On The Smart Home Industry". Forbes. Retrieved 2014-11-07.
19. ^ Mandula, K.; Parupalli, R.; Murty, C. A. S.; Magesh, E.; Lunagariya, R. (December 2015). "Mobile based home automation using Internet of Things(IoT)". 2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT): 340–343. doi:10.1109/ICCICCT.2015.7475301. ISBN 978-1-4673-9825-1. S2CID 14737576.
20. ^ Preville, Cherie (26 Aug 2013). "Control Your Castle: The Latest in HVAC Home Automation". ACHRNews. ACHRNews. Retrieved 15 Jun 2015.
21. ^ Asadullah, Muhammad (22 Dec 2016). "An Overview of Home Automation Systems". Conference Paper. IEEE. pp. 27–31. doi:10.1109/ICRAI.2016.7791223. ISBN 978-1-5090-4059-9.
22. ^ Jin, M.; Jia, R.; Spanos, C. (2016-01-01). "Virtual Occupancy Sensing: Using Smart Meters to Indicate Your Presence". IEEE Transactions on Mobile Computing. PP (99): 3264–3277. arXiv:1407.4395. doi:10.1109/TMC.2016.2684806. ISSN 1536-1233. S2CID 1997078.
23. ^ Jin, M.; Bekiaris-Liberis, N.; Weekly, K.; Spanos, C. J.; Bayen, A. M. (2016-01-01). "Occupancy Detection via Environmental Sensing". IEEE Transactions on Automation Science and Engineering. PP (99): 443–455. doi:10.1109/TASE.2016.2619720. ISSN 1545-5955. S2CID 4600376.
24. ^ Berger, Lars T.; Schwager, Andreas; Pagani, Pascal; Schneider, Daniel M. (February 2014). Smart Grid Applications, Communications, and Security. Devices, Circuits, and Systems. CRC Press. ISBN 978-1-4665-5752-9.