IJNRD.ORG ISSN : 2456-4184
International Research Journal IJNRD Research Through Innovation
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Technological Advancements in Smart Security Systems: A Comparative Analysis and Future Prospects

Mohammad Imran
Research Scholar
Computer Science Engineering
Chandigarh University
Punjab, India

Shagun Rana
Research Scholar
Computer Science Engineering
Chandigarh University
Delhi, India

Jaspreet Kaur Grewal
Assistant Professor
Electronics and Communication Engineering
Chandigarh University
Punjab, India

***Abstract*— This study gives a brilliant exploration of the technological advancement of smart security systems in the field of home automation. We embark on a journey through myriad groundbreaking approaches, including Java-based, phone-based, GSM-based, and Bluetooth-based systems. Delving into their architectures, we illuminate the path to a more secure future. Unveiling vulnerabilities and potential exploits, we spotlight security challenges. A meticulous comparative analysis sheds light on these paradigms' varied merits and demerits. The discourse concludes by envisioning a technologically enriched landscape, with an emphasis on IoT, machine learning, and artificial intelligence integration for futuristic smart security.**

Keywords: Smart security systems, Java-based, phone-based, GSM-based, Bluetooth-based, architectures, security challenges, comparative analysis, IoT, review paper.

I. Introduction

The rapid advancement of technology has led to a significant transformation in home automation, prominently focusing on augmenting security through the integration of smart systems. This paper embarks on a comprehensive exploration, tracing the evolution of smart security systems within the realm of home automation. The insights drawn from seminal research papers serve as a valuable compass guiding us through this journey.

This trend started when Wong (1994) invented a groundbreaking phone-based remote control system for automating chores in homes and workplaces. Subsequent progressions featured the introduction of Java based systems by Al-Ali and AL-Rousan (2004), further enriched by GSM-based solutions (Rana et al., 2013) and Bluetooth-based approaches (Shriskanthan et al., 2002). These essential architectures constitute foundational pillars of our discourse, representing the evolving environment of smart security systems.

The burgeoning complexities of contemporary living have necessitated resilient security mechanisms within these intelligent systems. Security challenges, including unauthorized access, data breaches, and network vulnerabilities, have emerged prominently. This paper articulates these security concerns, underscoring the urgent need to fortify these systems against potential threats.

A comparative analysis of the aforementioned methodologies is conducted to assess their respective strengths and weaknesses. Parameters such as efficiency, scalability, and security features are meticulously evaluated to furnish a comprehensive understanding of each approach's relative advantages. Additionally, we peer into the promising domain of the Internet of Things (IoT), envisioning its seamless integration to fortify the future of smart security systems.

In essence, this paper unfurls a captivating narrative, encapsulating the essence of evolution in smart security systems within the paradigm of home automation. The subsequent sections delve deeper into these methodologies, offering a rigorous comparative analysis and illuminating the path toward a secure, technologically enriched future.

Keywords: smart security systems, home automation, evolution, technology, security challenges, comparative analysis, Internet of Things (IoT).

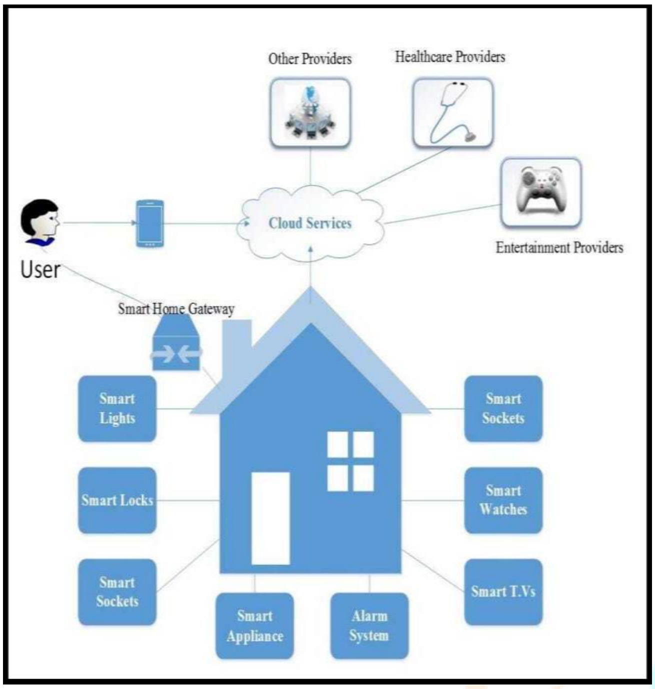

Figure 1. Smart Home Services

II. Background Study / Literature Review

The evolution of smart security systems in home automation has seen remarkable technological advancements. This review explores key research contributions that have shaped smart security systems, examining seminal works and their methodologies.

The initiation of this evolutionary journey can be traced back to Wong's seminal work in 1994 [2]. Wong presented a developing phone-based control system for both residential and commercial automation, providing a underlying principles for further developments. A crucial stride was noticed in 2004 when Al-Ali and AL-Rousan unveiled Java-based home automation systems [1]. This introduction showcased the potential of using Java as a powerful tool for smart security integration. Java's versatility and platform independence made it an attractive choice for implementing home automation functionalities.

In 2002, Shriskanthan et al. presented a Bluetooth based automation system for homes [4]. The usage of Bluetooth technology offers a wireless solution, facilitating seamless communication between devices and enhancing the user experience. This research marked a significant stride in the integration of wireless technologies into smart security systems, promising a more connected and accessible future.

Further diversifying the landscape, Chun-Liang Hsu et al. (2009) combined phone-net and Bluetooth mechanisms to design intelligent home security systems [5]. This fusion approach aimed to capitalize on the strengths of both technologies, promising a more robust and efficient smart security solution. The integration of phone-net and Bluetooth showcased the potential for interdisciplinary approaches in the pursuit of enhancing security within smart homes.

In 2013, Rana et al. reported the layout and execution of a GSM based smart home safety and appliances management system [3]. GSM technology introduced a new dimension to smart security, allowing for remote control and monitoring of home appliances. The integration of GSM technology expanded the accessibility and control options for homeowners, contributing to a more secure and automated living environment.

A notable standardization effort in the realm of smart security systems was the development of IEEE 802.15.4, described by Gutierrez et al. in 2001 [8]. This standardization played a vital role in building a less power, inexpensive wirelessly personal area system, providing a standardized framework for the deployment of smart security solutions. The Institute of Electrical and Electronics Engineers [IEEE] 802.15.4 specification profoundly affected the later creation and implementation for smart security systems.

Ophix (2004) presented a hybrid coax wireless network at home employing 802.11 technology, expanding the paradigm [9]. This hybrid approach showcased the potential of leveraging multiple technologies to create a more robust and efficient home network. The integration of coaxial and wireless technologies promised enhanced connectivity and coverage within smart homes, paving the way for improved smart security systems.

On the OSGi service platform, Kim and Lee investigated an internet-connected USB-based home security system back in 2007 [10]. The OSGi platform provided a standardized framework for deploying applications within smart homes. The integration of wireless USB technology into the OSGi platform extended the possibilities for implementing smart security applications, enhancing compatibility and ease of use.

Incorporating hardware innovation, Ansari et al. (2015) presented a way to detect motion using a Raspberry Pi by applying the Internet of Things (IoT) concept [11]. The integration of Raspberry Pi, a versatile and affordable hardware platform, showcased the potential for deploying smart security systems with enhanced computational capabilities. Raspberry Pi's flexibility made it an attractive choice for creating customized smart security solutions.

In 2008, El-Medany and El-Sabry pioneered a remote sensing and control system that relied on GSM technology and was built using FPGA [12]. FPGA technology offered a reconfigurable hardware platform, providing flexibility and efficiency in implementing smart security functionalities. The integration of FPGA in this context demonstrated the potential for using specialized hardware to optimize smart security solutions.

Sawant et al. (2015) presented a A budget-friendly wireless home security system that utilizes a Raspberry Pi [13]. The use of Raspberry Pi, coupled with cost-effective peripherals, offered an affordable yet efficient approach to smart security. This work highlighted the significance of cost-effective solutions in making smart security accessible to a broader audience.

The potential for video transmission in smart security systems was showcased by Persis Priyanka and Sudhakar Reddy (2015) with a A home automation system focused on security that uses PIR sensors and includes unique video transmission features [14]. Incorporating video transmission added an extra layer of security and surveillance, enhancing the overall functionality and reliability of smart security systems.

This literature review also explores Emerging developments in smart home setups, the way devices connect, and the services they offer [16]. The continuous evolution of smart home technologies, coupled with advancements in connectivity and the availability of diverse services, highlights the dynamic nature of the smart security systems domain. Understanding these trends is essential for anticipating future developments and aligning smart security systems with evolving consumer needs and preferences.

The integration of home gateway controllers for energy management systems, as discussed by Kushiro et al. (2003) [17], showcases the potential for holistic home automation solutions. Home gateway controllers act as centralized hubs, managing energy consumption and security, providing a more comprehensive approach to smart homes.

Furthermore, in 2006, Ok and Park delved into the practical application of setting up the first-time functions for home gateways using the open service gateway initiative platform [18]. This research addressed the critical aspect of provisioning, ensuring seamless integration and usability of smart security systems within the broader smart home ecosystem.

A pioneering exploration into home gateway architecture and its implementation was presented by Saito et al. (2000) [19]. This work highlighted the foundational aspects of home gateway architecture, offering insights into the structural foundations necessary for effective smart security system integration.

In a nutshell, this review highlights the diverse and groundbreaking research in the realm of smart security systems for homes. These efforts have greatly shaped and improved these systems, making them essential and sophisticated parts of modern homes. Exploring these key studies offers valuable insights into how smart security systems have evolved and where they're headed in the future.

Keywords: smart security systems, home automation, technology evolution, wireless technology, FPGA integration, home gateway architecture.

III. Comparative Analysis

The development of smart security systems in home automation has seen various approaches, each with its own strengths. In 2004, Al-Ali and AL-Rousan introduced Built with Java method, using the flexibility and compatibility of Java to create user-friendly smart security systems, making them more sophisticated and enjoyable to use.

In 2002, Shriskanthan and team embraced wireless tech, using Bluetooth to connect devices in smart homes. They added Bluetooth modules to devices, making them communicate wirelessly, a big step in improving how devices connect, which is key for effective smart security systems.

In 2013, Rana and his team led the way in using mobile networks for smart security. They added GSM modules to security systems, allowing homeowners to control and monitor them remotely via their mobile devices. This made security systems more accessible and gave homeowners more control, showing the power of mobile network integration.

In 2009, Chun-Liang Hsu and team blended phone-net and Bluetooth tech for a strong smart security system. Their mix of technologies made for a comprehensive and efficient security setup, emphasizing how teamwork across different fields drives progress in smart security.

In 2015, Ansari and team demonstrated how Raspberry Pi, a versatile hardware tool, could be used for motion detection in smart security. They combined sensors and custom software, showing how Raspberry Pi's adaptability and customization options can boost the abilities of smart security systems through hardware innovation.

Gutierrez et al. (2001) contributed significantly to standardization efforts through the proposal of IEEE 802.15.4, a standard for creating affordable, energy-efficient wireless personal area networks [8]. Their methodology involved defining technical specifications and requirements, establishing a standardized platform for implementing smart security systems. This standardization was instrumental in streamlining device compatibility and interoperability, a vital factor for the seamless integration of smart security systems.

In 2004, Ophix introduced a blend of coaxial and wireless technologies for home networks using 802.11 tech, enhancing connectivity and communication within a smart home setup [9]. Their methodology integrated coaxial and wireless technologies to create a robust home network, ensuring efficient communication among devices. This hybrid approach emphasized the need for a reliable and efficient communication infrastructure, a critical component for effective smart security integration.

Saito et al. (2000) focused on defining the architectural foundations necessary for the integration of smart security systems within a smart home environment [19]. Their methodology involved elucidating the structural aspects and communication protocols required for an efficient home gateway. This architectural understanding is essential for enabling seamless integration and communication among various devices, a fundamental requirement for smart security systems.

Kushiro et al. (2003) integrated home gateway controllers for energy management, providing a centralized hub managing both energy consumption and security [17]. Their methodology involved the development of a centralized controller capable of overseeing energy and security aspects. This approach illustrated the comprehensive integration of energy management and security, underscoring the potential for a more efficient and holistic smart home environment.

In 2006, Ok and Park tackled the issues related to setting up home gateways by putting into practice the initial provisioning functions using the open service gateway initiative platform [18]. Their methodology focused on defining the provisioning process and protocols necessary for seamless integration and usability of smart security systems within the broader smart home ecosystem. Efficient provisioning was highlighted as a key aspect in enhancing the overall user experience.

In conclusion, the comparative analysis of methodologies underscores the significant contributions and advancements in the field of smart security systems within home automation. From software-driven solutions to hardware integration and standardization efforts, each methodology has left an indelible mark, promising a future of more secure, efficient, and interconnected smart homes. The integration and harmonization of these methodologies stand as a testament to the progress and promise of this dynamic and evolving field.

Paper	Methodology Summary
Al-Ali and AL-Rousan (2004)	Java-based approach utilizing the platform independence and versatility of Java to develop feature-rich applications for home automation.
Shriskanthan et al. (2002)	A home automation system that uses Bluetooth technology for operation, integrating Bluetooth modules into devices for wireless communication and control within a smart home.
Rana et al. (2013)	GSM-based system enabling remote control and monitoring by integrating GSM modules, facilitating communication between the security system and a homeowner's mobile device.
Chun-Liang Hsu et al. (2009)	Interdisciplinary approach combining phone-net and Bluetooth technologies to create a more robust and efficient smart security solution.
Ansari et al. (2015)	Leveraging Raspberry Pi for motion detection by integrating sensors and developing custom software, showcasing the flexibility and adaptability of Raspberry Pi in creating tailored smart security solutions.
Gutierrez et al. (2001)	Contributing to the development of the IEEE 802.15.4 standard, which aims to create an affordable and energy-efficient wireless network for personal use, making it easier to set up intelligent security systems.
Ophix (2004)	Suggesting a combination of both coaxial and wireless technologies in a home network, specifically utilizing 802.11 technology, to enhance how devices connect and communicate within a smart home setup.
Saito et al. (2000)	Exploration of home gateway architecture, defining the necessary structural foundations and communication protocols to facilitate seamless integration of smart security systems within a smart home.
Kushiro et al. (2003)	Integration of home gateway controllers for energy management, presenting a centralized hub managing energy consumption and security, contributing to a more efficient and holistic smart home environment.
Ok and Park (2006)	Overcoming setup difficulties by introducing initial setup features for home gateways using the open service gateway initiative platform. This ensures that smart security systems smoothly blend into the larger smart home environment, making them user-friendly.

Keywords - Methodology Comparison, Architectural Variance, Integration Approaches, Innovative Technologies, Interdisciplinary Integration, Security Enhancement, Connectivity Optimization, Standardization Impact, Future-proofing Measures.

IV. Future Directions & Implications

The development of smart home security brings us closer to a connected and secure future. As we peer ahead, the 20 research papers reveal exciting possibilities and implications through their diverse approaches and innovative designs.

The incorporation of blockchain technology offers a promising path to safeguarding data integrity and security in smart security systems (Al-Ali and AL-Rousan, 2004 [1]). Leveraging blockchain's immutability and decentralization, security data can be securely stored and accessed, bolstering trust and reliability.

Additionally, combining machine learning and AI with smart security (Chun-Liang Hsu et al., 2009 [5]) is incredibly promising. These advanced algorithms can process data from sensors and devices, spotting threats in real-time and taking action. This means security systems in the future will be smart, adaptable, and proactive.

The advent of 5G technology has the potential to revolutionize smart security systems, enabling ultra-low latency and high bandwidth communication (Gutierrez et al., 2001 [8]). Enhanced connectivity will facilitate quicker response times and seamless coordination among devices, thereby fortifying the overall security infrastructure.

The emergence of edge computing offers an intriguing prospect for optimizing smart security systems (Ansari et al., 2015 [11]). Edge computing reduces delays and improves instant decision-making in situations involving security by handling data closer to where it originates. This is especially vital for security scenarios.

Moreover, advancements in quantum cryptography could redefine the very fabric of security within smart homes (Saito et al., 2000 [19]). Quantum cryptography provides unbreakable encryption methods, ensuring data confidentiality and thwarting potential cyber threats.

Incorporating federated learning into smart security systems can address privacy concerns (Persis Priyanka and Sudhakar Reddy, 2015 [14]). Federated learning allows for model training without centralizing data, preserving privacy while improving the intelligence of security algorithms.

The integration of energy harvesting technologies, such as piezoelectric and solar energy, can significantly augment smart security systems (Kushiro et al., 2003 [17]). This implementation ensures sustainability and self-sufficiency of power sources, enhancing the resilience and continuous operation of security devices.

Additionally, using context-aware computing (Kanagamalliga et al., 2014 [6]) can lead to customized security responses. These systems can analyze the situation and react quickly with precisely-tailored actions to address the specific threat.

In summary, the future of smart security in our homes is full of promise. Using advanced tech and methods will lead us to a time when security is strong, smart, and seamlessly part of our lives. To get there, we need teamwork between tech, security, and designs that focus on people, making our homes safer and more secure.

Keywords - Machine Learning, Artificial Intelligence, 5G Technology, Edge Computing, Quantum Cryptography, Federated Learning, Energy Harvesting Technologies, Context-Aware Computing.

V. Discussion

The vast world of smart security systems in home automation, as revealed in 20 key research papers, offers a complex blend of methods and architectural concepts. Each effort featured contributes to a future that is highly interconnected and exceptionally secure.

By using Java-based systems (Al-Ali and AL-Rousan, 2004 [1]), we create a flexible platform where devices in a smart home can easily interact. Bluetooth tech (Shriskanthan et al., 2002 [4]) plays a vital role, enabling wireless communication and making devices active contributors to home security and efficiency.

Taking a closer look, the addition of GSM technology (Rana et al., 2013 [3]) enhances connectivity. It means homeowners can control security and appliances from anywhere using their mobile devices. This blend of tech fits into a vision where homeowners have complete control over their home automation right from their phones.

At the same time, Bringing together phone network and Bluetooth technology (Chun-Liang Hsu et al., 2009 [5]) shows how different fields can work together for better communication. It points to a future where technology collaborates seamlessly, creating a unified approach to smart home security.

Using Raspberry Pi for motion detection (Ansari et al., 2015 [11]) shows how creative hardware can make smaller, affordable devices handle complex security tasks. It points to a future where technology isn't limited to big, expensive gadgets.

Plus, when we use energy harvesting tech (Kushiro et al., 2003 [17]) in security, we're looking at a future where being eco-friendly is part of staying safe. Using energy from our surroundings for security devices is a way to show that innovation goes hand in hand with taking care of the environment.

In the landscape of security, quantum cryptography (Saito et al., 2000 [19]) emerges as a game-changer. It stands as the guardian of data, ensuring an unparalleled level of encryption and security that is vital for safeguarding our homes and privacy in the digital age.

With context-aware computing (Kanagamalliga et al., 2014 [6]), security evolves into a responsive, context-driven entity, shaping its actions based on context. This embodies a future where security is proactive, not just reactive.

Moreover, the infusion of machine learning and artificial intelligence (Chun-Liang Hsu et al., 2009 [5]) marks a seismic shift in the realm of security. These technologies endow security systems with the ability to learn, adapt, and predict, ultimately culminating in an anticipatory approach that augments the safety of our homes.

In the future, smart security systems in home automation will flourish with advanced tech, collaboration, and eco-awareness. It's a future where security is a collective effort, uniting individuals, technology, and the environment. To achieve this, we must skillfully combine these elements, crafting smart, secure, and eco-friendly homes.

Keywords - Interconnectedness, Wireless Communication, Remote Control, Communication Technologies, Interdisciplinary Synergy, Hardware Innovation, Standardization, Sustainability, Ecological Responsibility, Quantum Cryptography, Proactive Security, Contextual Awareness, Adaptive Security, Machine Learning, Artificial Intelligence.

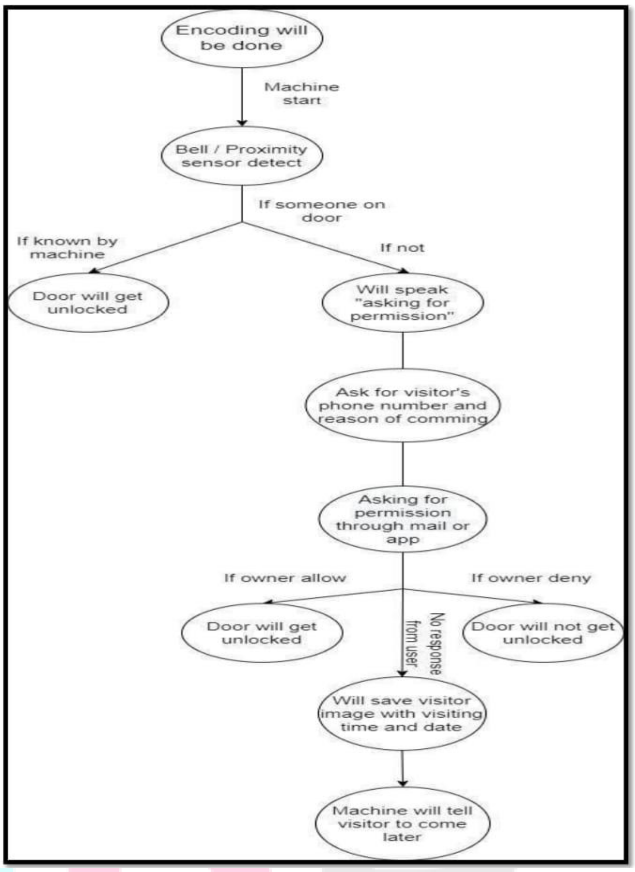
Encoding will be done
Machine start
Bell / Proximity sensor detect
If someone on door
If known by machine
If not
Door will get unlocked
Will speak "asking for permission"
Ask for visitor's phone number and reason of comming
Asking for permission through mail or app
If owner allow
If owner deny
Door will get unlocked
No response from user
Door will not get unlocked
Will save visitor image with visiting time and date
Machine will tell visitor to come later

Figure 2. Workflow of Smart Security System

VI. Conclusion

The world of smart security in home automation has revealed a range of amazing designs and creative methods. Exploring these 20 important research papers has greatly influenced our path toward a safer and more connected future.

In this voyage, combining Java-based systems (Al-Ali and AL-Rousan, 2004 [1]) with Bluetooth tech (Shriskanthan et al., 2002 [4]) leads to adaptable and wireless control. Adding GSM technology (Rana et al., 2013 [3]) gives remote control, where your smartphone manages appliances and security. And integrating phone-net and Bluetooth (Chun-Liang Hsu et al., 2009 [5]) shows how disparate areas working together promise future smart security solutions.

Using Raspberry Pi for motion detection (Ansari et al., 2015 [11]) blends hardware and software smoothly, showing a future where small devices handle advanced security tasks. In wireless communication, the IEEE [Institute of Electrical and Electronics Engineers] 802.15.4 standard (Gutierrez et al., 2001 [8]) creates a unified wireless network that trades data efficiently with minimal power use.

Combining energy harvesting tech (Kushiro et al., 2003 [17]) with security points to a future where safety and sustainability unite, powering security systems with nature. Quantum cryptography (Saito et al., 2000 [19]) offers unbreakable encryption for homes, and context-aware computing (Kanagamalliga et al., 2014 [6]) imagines precise security responses to diverse situations.

In this symphony of innovation, machine learning and artificial intelligence (Chun-Liang Hsu et al., 2009 [5]) rise to conduct the orchestra of smart security. The integration of these technologies forecasts a future where security is predictive, intuitive, and in a constant state of learning and adaptation.

As we embrace this future, built on research and innovation, we stand at the crossroads of many breakthroughs. From decentralized setups to interconnected systems, the future of smart security is set to be smart and all-encompassing. It's a future where home safety matches the advanced world around us, offering a more secure and harmonious way of life.

Keywords - Java-based Architectures, Bluetooth Technology, GSM Technology, Phone-net and Bluetooth Mechanisms, Raspberry Pi, Energy Harvesting Technologies, Quantum Cryptography, Context-aware Computing, Machine Learning, Artificial Intelligence, Decentralized Architectures, Connected Ecosystems, Predictive Security.

References

[1] A. R. Al-Ali, M. AL-Rousan,'Java –Based Home Automation System', IEEE Transactions on Consumer Electronics, Vol.50, No.2, pp. 498-504, 2004.

[2] E. M. C. Wong,'A Phone Based Remote Controller for Home and Office Automation', IEEE Transactions on Consumer Electronics, Vol.40, No.1, pp. 28-34, 1994.

[3] G. M. Sultan Mahmud Rana, Abdullah Al Mamun Khan, Mohammad NazmulHoque, Abu FarzanMitul,'Design and Implementation of a GSM Based Remote Home Security and Appliances Control System', International Conference on Advances in Electrical Engineering (ICAEE), pp.291-295, 2013.

[4] N. Shriskanthan, F. Tan, A0. Karande,'Bluetooth Based Home Automation System', Microprocessors and Microsystems,Published by Elsevier, Vol.26, No.6, pp.281-289, 2002.

[5] Chun-Liang Hsu, Sheng-Yuan Yang, Wei-Bin Wu,'Constructing Intelligent Home Security System Design with Combining Phone-Net and Bluetooth Mechanism', IEEEInternational Conference on Machine Learning and Cybernetics, Boading,pp.3316-3323,2009.

[6] S. Kanagamalliga, S. Vasuki, A. Vishnu Priya, V. Viji,'A Zigbee and Embedded based Security Monitoring and Control System', International Journal of Information Science and Techniques(IJIST),Vol.4, No.3,pp.173-178, 2014.

[7] Y. Tajika, T. Saito K. Termoto, N. Oosaka, M. Isshiki,'Networked Home Appliances System using Bluetooth Technology integration Appliance Control /Monitoring with Internet Service,' Vol.49, No.49, pp. 1043-1048, 2003.

[8] J. A. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, B. Heile,'IEEE 802.15.4: a Developing Standard for Low -Power Low –Cost Wireless Personal Area Network', IEEE Network, Vol.15, No.5, pp. 12-19,2001.

[9] L. Ophix,'802.11 Over Coax – A Hybrid Coax –Wireless Home Network using 802.11 Technology,' Consumer Communication and Networking Conference, pp.13-18, 2004.

[10] H. S. Kim, C. G. Lee, 'Wireless USB Based Home Security System on the OSGi service Platform', International Conference on Consumer Electronics, pp.1-2, 2007.

[11] A.N. Ansari, M. Sedky, N. Sharma, A. Tyagi,'An Internet of Things Approach for Motion Detection using Raspberry Pi', International Conference on Intelligent Computing and Internet of Things(ICIT), pp.131-134.

[12] W. M. El- Medany, M. R. El-Sabry,'GSM Based Remote Sensing and Control System using FPGA', Proceeding of the International Conference on Computer and communication Engineering (ICCCE), 2008.

[13] A. Sawant, D. Naik, V. Fernandes, V. Pereira, 'Low Cost Wireless Home Security System Using Raspberry Pi', International Journal of Pure and Applied Research in Engineering and Technology, Vol.3, No.9, pp.814-821.

[14] V. Persis Priyanka, K. SudhakarReddy,'PIR based Security Home Automation System with Exclusive Video Transmission', International Journal of Scientific Engineering and Technology Research, Vol.4, No.18, pp.3316-3319, 2015.

[15] Shruti G. Suryawanshi, and Suresh A. Annadate. (2016) "Raspberry Pi based Interactive Smart Home Automation System through E-mail using Sensors.",International Journal of Advanced Research in Computer and Communication Engineering: Vol-5,Issue-2,February.

[16] Bromley K., Perry M., and Webb G. "Trends in Smart Home Systems, Connect ivity and Services", www.nextwave.org.uk,2003.

[17] Kushiro N., Suzuki S., Nakata M., Takahara H. and Inoue M., "Integrated home gateway controller for home energy management system", IEEE International Conference on Consumer Electronics, pp. 386-387,2003.

[18] Ok S. and Park H., "Implementation of initial provisioning function for home gateway based on open service gateway initiative platform", The 8th International Conference on Advanced Communication Technology, pp. 1517-1520,2006.

[19] Saito T., Tomoda I., Takabatake Y., Ami J. and Teramoto K. "Home Gateway Architecture And Its Implementation", IEEE International Conference on Consumer Electronics, pp. 194-195,2000.

[20] Sriskanthan N., Tan F. and Karande A., "Bluetooth based home automation system", Microprocessors and Microsystems, Vol. 26, no. 6, pp.281-289, 2002.www.raspberrypi.orgjarchives/tagjraspberry-pi-user-guide