International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

An Enhanced Methodology on Internet of Things with Cloud in Smart Electrical Systems

Kiran Kumar Vadlamudi, Ch. Ravi Kumar

Abstract: ***The smart management system plays a vital role in many domains and improves the reliability of protection and privacy of a system. Electrical systems have become a part in everyday human life. The next generation electrical systems will entirely depends on fully automated and smart control systems. In the present paper various mechanisms of cloud gateways and security issues are explored for smart management of an electrical system. The present survey work is reconnoitred with Internet of Things (IoT) in association with cloud. Cloud based IoT in smart electrical system provides potential enhancement of performance, management, and resilience of the smart system. However, the espousal of cloud based IoT system in smart electrical system to store and retrieve the data from cloud may increase risks in data privacy and security. Despite the different flaws in global integration of cloud with IoT through internet, various end-to-end security schemes are discussed to overcome these flaws. As a result in many of the applications easy IoT cloud gateway along with homomorphic encryption technique is set up to solve communication overheads and security issues.***

Keywords: smart electrical system, privacy, IoT, cloud, security

I. INTRODUCTION

The daily human life includes many electrical appliances. Without electrical devices it is hard to imagine one's comfortable life. But, the misuse of those electrical devices may cause waste of energy which may indirectly cause of raise in green house gaseous. Efficient energy utilization is very important in the present world. This demands automatic device maintenance and controlling. The device maintenance need through data recording for processing the data. In the recent days the recording or storage of data is done through cloud inorder to reduce the infrastructure cost. At the same time the cloud also demands the security concerns. In the present research work the IoT is used to bring all the electrical appliances in a smart building onto a single network. The operations and status of the appliances are monitored by IoT device with the help of several sensors like temperature, light, Ultrasound sensors, humidity sensors, and etc.In the present system, an energy meter is used to calculate the total power consumption and also individual power consumption occurred due to various electrical devices. Based on the energy meter measurements one can analyse their usage in their premises. It is also very important to monitor daily consumption inorder to take wise decision for their firm or house. This can be achieved by storing all the electrical gadget information in a cloud.

A cloud allows a person (site engineer/house owner/ CEOs/..) to monitor electrical device status of their premises remotely. Hence with the base of this cloud information the engineer can take a wise decision to change the status of the electrical device. The person can send control signal to the field with the help of internet.

When internet come into the picture there is a lot of chances of hackers. It is very important to protect the data to avoid unauthorised intrusions. In the present paper different cloud security systems are discussed to protect the customer data in the direction of protecting their privacy and safekeeping of their authentication.

1.1 Internet of Things

Internet of Things (IoT) refers to the stringent connectedness between digital and physical world. Many researchers defined IoT as, "A global infrastructure for the information society enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies" [1][2]. Many studies analysed that at the beginning of next decade around 20 billion devices will be interfaced and under the control of internet [3]. This revealed that efficient technology is required to manage devices via internet. It has been observed that Internet of Things is a branch of science effectively involved in handling virtual devices and made ease of accessing those devices with sensor cloud, virtual memory through various pre-defined services. The IoT spreading its wings in every domain such as transportation, e-commerce, hospitals, patient diagnosis, weather monitoring, industrial and home appliance monitor and control, defence, robotics, artificial intelligence, business process management, control process instrumentation, smart city, smart home, smart grid and not limited to these areas [4]. Various applications of IoT are shown in figure 1.

Manuscript published on 30 September 2019
* Correspondence Author
Mr. Kiran Kumar Vadlamudi*, Research Scholar, Department of EEE, College of Engineering and Technology, Acharya Nagarjuna University, India. Email: kiran.vk211@gmail.com
Dr. Ch. Ravi Kumar, Assistant Professor, Department of EEE, College of Engineering and Technology, Acharya Nagarjuna University, India
Email: ravikumarchekka@gmail.com

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

Figure 1 various domains of IoT

1.2 Process of IoT

An IoT is a system which provides services like sensing, publishing data to subscriber, sniff the publishing data and distribute the data to subscriber, storing and retrieving the data, and accessing the data from web apps. In the IoT systems the sensors initially sense the physical parameters and then transducers convert them into electrical signals. The electrical signals further converted into digital signals with the help of Analog to Digital Converters (ADC). In recent systems the microcontrollers are designed with inbuilt ADC and pulse width modulations for sampling the input signal. The publisher cast the sensing data to all subscribers. The broker in between publisher and subscriber act as mediator. The mediator here will drive the sensing events to the destination. The subscribers are the devices which are requested for the sensing input. The subscribers use learning algorithms to take intelligent predictions to take wise decision in correct time. The processing of algorithms can be done at either client location or at cloud. In most of the time the cloud is also used to store the publishing data. In the recent days almost all domains are depending on IoT technology and processing large data. Hence cloud services are required to process and store large data. The security is main concern in the cloud as the data is available publicly. Hence some encryption mechanisms' are required while using cloud based IoT. The encryption can be done before publishing the data into cloud or encryption can also be done at cloud based on the requirement and system design environment.

With all these concerns the IoT system requires the following fundamental devices to resolve many of the traditional system errors and flaws. Such as,

1. Sensors
2. IoT integrating modules
3. Gateway
4. Internet connectivity
5. Memory storage and their interface
6. Display interfaces mostly Apps

The exact state of IoT is state based on the device coordination and integration of new devices [5]. The IoT not only integrated with new devices to offer new services it also provides new services with independent features [6,7]. Along with the benefits offered by multiple newly integrated devices, it is also highly essential to concentrate on the obstacles come across in the data management and device management [8].

Some of the challenges need to be observed in IoT based systems are:

i. Device Management: In IoT based system wide variety of devices and numerous devices are integrated on the network. There is a big challenge of making appropriate controlling these devices in terms of traffic control, memory management, and managing diversified devices. Hence an efficient protocol is required for efficient management of these devices [9][10].

ii. Data management: The data is integrated from several devices and systems like multiple servers, sensors, internet devices, and processors. Here a large volume of data management is a big issue need to be faced and increasing its facets day-by-day as the network increases by interconnection devices. An optimized data evaluation and synthesis is required from the large volume of data produced in the IoT based system. The synthesis is required inorder to segregate, analyse, and compare the collected data to obtain a meaning full data for processing [9].

iii. Security: In the recent days it is observed that the number of interconnecting devices is increasing in an organization, or city, or world-wide is increasing. As the number of interconnect devices increases the security concerns also increases in this proportion. Many devices are connected on IoT network with different protocols, and work under different environments, and process different types of data. The strategic situations like the above said are alarming the present system to concentrate more on security issues. The nonexistence of encryption or inefficient encryption also may drastically increase security challenges [11]. The recent analysis revealed that, in near future the number of IoT devices will cross more than 20 billion. So, in proportion the security challenges are also increases which require deep concern [9]. The strategic environment contains sensitive data require more security for instance like smart grid applications.

iv. Privacy: The privacy mainly concerns about the personal information. Such as personal tariff usage, bill payments, usage and real time work load are some important information required to be hide from other parties of smart grid system. This is a biggest challenge that requires at most priority to be given in the smart electricity system [9, 12]. Some IoT service providers require some data like tariff usage, and bill details based on which third parties can provide best services and offers to their customers. Beside these services depend on the customer data, some data such as in-out time, vehicle details, health, and financial information highly need privacy which are not willing to share by the customer or user [9]. Figure 2 is showing an architecture of IoT based system. The figure is depicting how a user interacting with IoT system. The IoT system transacts with the sensors and uploads it to cloud. To provide the security and to hide from the third party the sensory data first encrypted and then sent to the cloud. The user can monitor and manage the cloud data remotely with web applications or mobile apps. The user can send the commands to actuators through cloud. The cloud retains the data after encryption. The cloud data is given to actuators after decryption. With all the above issues and concerns such as data and device management services, data integrity, privacy and security are all can be overcome with an efficient IoT system in association with cloud.

The IoT system with cloud also increases reliability, scalability, and number of services. The next section elucidates the cloud organization and management with respect to the Internet of things.

II. CLOUD COMPUTING IN IOT

The cloud is pool of shared resources provides services on demand to the subscribers [13][14]. The infrastructure required to support for providing services to the subscribers is referred as cloud [14][15]. The fundamental services provided by cloud are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure as a Service (IaaS).In the current work, device monitoring, consumption monitoring and controlling applications SaaS will satisfy the project needs.

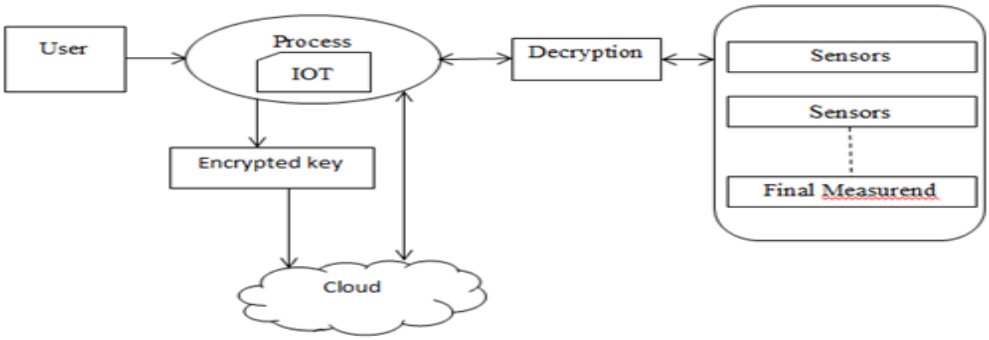

Figure 2 A framework of Cloud based IoT system

In SaaS model user or developer need not to develop any softwares or install the softwares. Hence the clients need not to have any bothering of managing the softwares. The SaaS model includes different types of software modules and they are utilised whenever and wherever they are demanded by the user [14]. Finally, the cloud provides large database to store different customer data, efficiently, flexibly, with high stability and scalability at low cost. The cloud in IoT minimizes the relative error and increases the accuracy [16][17].

2.1. Smart Building

A smart building consists of different number of electronic devices and sensors acts in different environments and applications with several communication protocols [18]. These smart systems make home environment more comfortable space for living. The smart systems will provide controlling the home appliances and can be switch off them whenever they are not required for service. Anyone can know what is happening at home from remote locations and can take necessary actions on home appliances. However the home automation systems provides more flexible operations and features it has its own constraints such as security issues. The security issues are discussed later in the next section. In the next section the existing protocols and related works are discussed in brief.

2.2 Concerns in Cloud Computing

Data security has become the priority consideration for the designing of every IoT network systems. Computer-controlled devices in automobiles and electrical appliances have been shown to the vulnerable to attackers who have access to the network. Because the IoT is a rich source of data it will always be vulnerable to sophisticated attacks. Different entities in the smart grid system, such as smart grid operators and cloud service providers who collect and manage home appliance utilisation information, can obtain more specific details about consumers' lifestyles (e.g. attendance and leave times, activities and even utilities used) Some of the other concerns are listed below

i) Inadequate physical security for interconnected devices
ii) Insecure Web interfaces
iii) Insecure software/firmware
iv) Insecure mobile interfaces
v) Insecure network services
vi) Insecure transport and transmission
vii) Inefficient authorization and authentication
viii) Privacy and confidentiality concerns
ix) Data integrity concerns

III. EXISTING PROTOCOLS

The merits and demerits of various existing techniques and schemes of protocols are discussed which will help the future researchers to understand research problems and well-designed solutions. Along with the pros and cons various coordination present in the existing systems' designs and logic implementations are discussed in the present paper. As in the present work the IoT applications are discussed with respect to the smart home or smart building systems, the widely used features and protocols used in smart buildings are discussed. The fundamental issues related to the current theme are discussed in this section.

3.1 Thin Servers

The main objective of the embedded thin servers is to detach the infrastructure and applications. This can happen by sharing the devices or things on the web through internet, technologies, protocols such as http (hypertext transfer protocols) and REST (Representational State Transfer) [19,20].

This approach will help the designers to integrate more number of devices and allows interfacing remote devices with more flexibility. This also makes easy to develop new application with ease of operations. The hardware design patterns become more flexible with embedded thin servers.

As the number of things increases in the IoT network the network size also increases in proportional to the number of devices.

This will increase the network size and production of data and consumption of data become very tedious job in complex networks. The optimization of energy consumption is also one of the biggest challenges in the recent trends.

3.2 Design patterns

The self-organised network node consumes less power and occupies less memory with centralised memory system.
The wireless network systems are efficient with advanced protocols such as Bluetooth, ZigBee, Highway Addressable Remote Transducer (HART), IEEE 802.15.4, and 6LoWPAN [21]. Hence an efficient hardware and software design patterns are highly essential inorder to develop energy efficient systems. The software design patterns are needed to be developed in such a fashion that they are reusable in similar problems [22]. The design patterns are developed based on the type of problem, type of system. It creates the abstraction of the given problem and follows all design and development features.

3.3 ZigBee Gateways

ZigBee is one of the wireless topology widely used in wireless smart building systems. The ZigBee provides good solution for smart buildings to accomplish best operations when compared with the existing technologies [23]. Different types of sensors and devices are interfaced in smart building system. Hence different technologies are used to operate all these smart devices in home or building automation system. Hence an effective gateway system must present in IoT based automation system to handle and synchronize variety of technologies.
ZigBee will play very important role when more than one network is interconnected in smart control systems. The ZigBee will help in synchronizing the protocols, devices, making compatible of technologies, and schemes of one network with other network. Not only the gateway used for compatibility of devices and technologies used in the interconnection, it can also be used to integrate parts of the network which is present in the IP networks and in the internet. The Bjelica designed a network with gateway which allows to integrate IPV6 devices with the help of 6LoWPAN protocol [24]. This system helps in searching the devices and integrating them in the network. After the devices are identified it establishes a communication with the server cloud.

3.4 Cloud gateways

There are some efficient systems effectively involved to overcome the problems recognized in the existing cloud models. Several existing systems mostly involved in smart home/building are discussed in the following section.

3.4.1 Intel IoT

The Intel IoT is developed to integrate devices and makes different technologies compatible on the network system. It also used to upload the sensory data onto the cloud and also able to provide the analysis of results. The Intel IoT platform has dedicated hardware that collects the data and uploads to cloud. It consists of software which will present the result after analysis of the data. Hence the Intel IoT provides a platform which will helpful to upload the data into cloud and access the data from cloud, finally analyses the cloud data.

3.4.2 IFTTT

The full form of IFTTT is “If this then that”. The IFTTT provides a service called event-based programming. It helps the users to interact the devices present on the system network using event based programming. The event based programmers allows the programmers to reschedule the modules to execute when an event occurs. Although the IFTTT is not developed for home automation, a user can use this for smart buildings, as actions are triggered after an event occurs. But, the user can not extend the services to the new devices.

3.4.3 EasyIoT

The main objective of EasyIoT is to provide interface between users and devices. Unlike IFTTT it uploads the device data to the cloud. The physical devices are managed and controlled by web interface.

IV. SECURITY

Hence most of the gateways allow accessing the device information, data, and system features through cloud. As the number of devices increases then the cloud dependency also increases in proportion. The cloud computing has its own disadvantages in storing and retrieving retained data. One of the biggest challenges of cloud is storing large data, as the number of devices connected to internet increasing day by day. Security is one-more biggest problem now-a-days in cloud; everybody is facing many challenges in almost all organizations and in our daily life due to cloud.
The information should be stored in secure place and must available to public subscribers. The information is stored in such a way that the device data should only be available to authorised persons or objects only. The gateway also helps here in differentiating appropriate subscribers.

In order to provide a more cost-effective and efficient computer-controlled environment a robust IoT Security Management System (IoTSMS) needed that enables the seamless integration of new applications that typically require installation of relevant devices, sensors and software. The IoTSMS must be able to handle a large number of devices, interconnected systems, transmission and processing of the pertaining security data.
There is no standard proposed IoTSMS for developing integrated solutions and incorporating new applications to cast an efficient, strong and sustainable security in the IoT environment. To fill this gap an efficient security model is required for robust IoTSMS.

4.1 Various end-to-end security schemes

i. Homomorphic Encryption technique: Very high complicated calculations are included in this encryption system. The cost of computing and the storage is very high. It avoids communication overheads.[25]
ii. Encrypted Search and Database: Encrypted search is the one of the most common operation.
Encrypted search is a lightweight mechanism for database encryption. It is an asymmetric encryption mechanism for databases in the cloud. The private/public key order is very useful for decryption/encryption when the commutative encryption is applied more than once on to the data. [25]
iii. Hybrid Technique: This uses both the authentication and key sharing techniques.

By making process more secure, powerful key sharing and authentication process are used. [25] [26]

iv. Distributive Storage: Distributive storage of data is one of the promising approach in the cloud environment. Internal or external data are divided into chunks to protect them from unauthorized access. The maximum security can be achieved by dividing the user's data into pieces. [26] [27]

v. Data Concealment: Data concealment is also be used to keep the data confidentiality in the cloud environment. The data concealment concept is introduced for database security. This technique will combine the real data with the visual fake data to make real data as the negative (false) one. The overall volume of real data can be increased by Data concealment but it provides enhanced security for the private data. [27]

V. CONCLUSION

In the domain of IoT many smart home and smart building systems are existed but failed to integrate their technologies and devices from one system network to another system network. This will increase the system cost and time complexity. This will have a great impact on scalability of cloud based IoT. Due to the limitations of protocols used in integration of devices connected on internet, an efficient gateway is required in order to integrate and make compatibility with the existing and new devices and technologies. The gateway not only optimizes the compatibility but also increases the reliability and production cost of the internet devices. The level of security in cloud will be increased with encrypting the data. The data security is increased by encryption and it is decrypted back to make the data understandable by the user and the actuators. The security in the cloud improves the consumer trust on cloud service. The easy IoT establishes connection between physical devices and web applications. In multi storied buildings the IoT Security management system is monitored by various end-to-end security schemes. The main advantage of easy IoT is, it directly uploads the data to cloud. Although the cost of computing is high with Homomorphic encryption technique, it is one of the mostly preferred techniques as it overcomes the communication overheads.

REFERENCES

1. L. Atzori et al., "The internet of things: A survey", Comput. Netw., vol. 54, no. 15. pp. 2787–2805. 2010.
2. Andrea Zanella et al., "Internet of Things for Smart Cities", IEEE Internet of things journal. Vol. 1. No. 1. Feb 2014. pp 22-32.
3. http://www.gartner.com/newsroom/id/2905717 [Accessed on 28 Nov, 2018].
4. Kuchi N S S S S Utpala et al., "Authenticated IoT Based Online Smart Parking System with Cloud", Pramana Research Journal, Vol 9 no 4, 2019.
5. I. Lee and K. Lee. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4):431–440, 2015.
6. V. Stirbu. Towards a RESTful plug and play experience in the Web of Things. Proceedings – IEEE International Conference on Semantic Computing 2008, ICSC 2008, pages 512–517, 2008.
7. K. Bing, L. Fu, Y. Zhuo, and L. Yanlei. Design of an Internet of things-based smart home system. Proceedings of the 2nd International Conference on Intelligent Control and Information Processing, ICICIP 2011, (PART 2):921–924, 2011.
8. Y.-K. Chen. Challenges and opportunities of internet of things. 17th Asia and South Pacific Design Automation Conference, pages 383–388, 2012. ISSN 2153-6961. doi: 10.1109/ASPDAC.2012.
9. E. Borgia. The Internet of Things vision: Key features, applications and open issues. Computer Communications, 54:1–31, 2014.
10. B. Pramod Kumar et al., "Intelligent Network Design of intelligent multinode Sensor networking", IJCSE, vol. 2, no. 3, 2010.
11. D. Bradley, D. Russell, I. Ferguson, J. Isaacs, A. MacLeod, and R. White. The Internet of Things – The future or the end of mechatronics. Mechatronics, 27:57–74, 2015.
12. M. O'Neill. The Internet of Things: do more devices mean more risks? Computer Fraud & Security, 2014(1):16–17, 2014.
13. S.Renuka et al., "Statistical Accuracy of Authentication with Biometrics", International Journal of Engineering and Advanced Technology (IJEAT), Vol 8 (4), April, 2019, pp 1040-1043.
14. S. Renuka et al., "A Survey on Cloud Data Security", International Journal of Computer Sciences and Engineering, Vol.7, Issue.4, 2019 pp.88-95.
15. Y. Y. Y. Yang, Z.W. Z.Wei, D. J. D. Jia, Y. C. Y. Cong, and R. S. R. Shan. A Cloud Architecture Based on Smart Home. Education Technology and Computer Science (ETCS), 2010 Second International Workshop on, 2(60970130):440–443, 2010. doi: 10.1109/ETCS.2010.293.
16. N. Suresh Kumar et al., "Digital frequency meter using DMA Terminal Count stop method", IJET, vol. 2, no. 2, pp. 34-37, 2010.
17. N. Suresh Kumar et al., "A New Method to Enhance Performance of Digital Frequency Measurement and Minimize the Clock Skew", *IEEE Senso Journal*, vol. 11, no. 10, pp. 2421-2425.
18. C. Lee, L. Zappaterra, K. Choi, and H.-A. Choi. Securing smart home: Technologies, security challenges, and security requirements. 2014 IEEE Conference on Communications and Network Security, pages 67–72, 2014.
19. M. Kovatsch, S. Mayer, and B. Ostermaier. Moving Application Logic from the Firmware to the Cloud: Towards the Thin Server Architecture for the Internet of Things. 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pages 751–756, 2012.
20. B. Ostermaier, M. Kovatsch, and S. Santini. Connecting things to the web using programmable low-power WiFi modules. Proceedings of the Second International Workshop on Web of Things - WoT '11, pages 1–6, 2011.
21. P. P. Pereira, J. Eliasson, R. Kyusakov, J. Delsing, A. Raayatinezhad, and M. Johansson. Enabling Cloud Connectivity for Mobile Internet of Things Applications. 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering, pages 518–526, 2013.
22. D. Gay, P. Levis, and D. Culler. Software design patterns for TinyOS. ACM Transactions on Embedded Computing Systems, 6(4):40–49, 2007.
23. W. S. Lee and S. H. Hong. KNX - zigbee gateway for home automation. 4th IEEE Conference on Automation Science and Engineering, CASE 2008, pages 750–755, 2008.
24. M. Z. Bjelica, B. Mrazovac, N. Teslic, I. Papp, and D. Stefanovic. Cloud-enabled home automation gateway with the support for UPnP over IPv4/IPv6 and 6LoWPAN. IEEE International Conference on Consumer Electronics, (3):520–521, 2012.
25. Abdulatif Alabdulatif et al., "Privacy-preserving cloud-based billing with lightweight homomorphic encryption for sensor-enabled smart grid infrastructure", IET Wireless Sensor Systems, july 2017.
26. Claude Castelluccia, "Efficient and Provably Secure Aggregation of Encrypted Data in Wireless Sensor Networks", ACM Transactions on Sensor Networks, Vol. 5, No. 3, Article 20, May 2009.
27. Paria Jokar et al., "A survey on security issues in smart grids", Security and communication networks, Security Comm. Networks (2012)

AUTHORS PROFILE

Kiran Kumar Vadlamudi has received the B-Tech degree in Electrical and Electronics Engineering from Jawaharlal Nehru Technological University Hyderabad, India and M.Sc in Embedded Systems and Control from University Of Leicester, UK and currently pursuing his Ph.D from Acharya Nagarjuna University, Guntur, India. He worked as an Asst. Professor in Electrical and Computer Engineering Department in Mizan-Tepi University, Ethiopia. His areas of interest were electrical machines Control, Embedded systems and Control, IoT and Cloud Computing.

Ch. Ravi Kumar has received the B.Tech degree in Electrical and Electronics Engineering from A.S.R.College of Engineering and Technology, Tanuku in 2003 and M.tech degree from JNTU Anantapur, A.P.-India in 2005. He completed his PhD from Acharya Nagarjuna University in 2017. Currently he is working as Asst.Professor in University college of Engineering and Technology, Acharya Nagarjuna University, Andhra Pradesh India. His areas of Interest are Power system operation and control, optimization techniques, fractional order controllers