Digital Object Identifier:10.11989/JEST.1674-862X.80716117

Technical Analysis of Security Management in Terms of Crowd Energy and Smart Living

MD Shahrukh Adnan Khan* | Muhammad Ahad Rahman Miah | Shaikh Rashedur Rahman | Mirza Mursalin Iqbal | Aseef Iqbal | Aravind CV | Chua Kein Huat

Abstract—In this paper, a technical and statistical analysis of security system and security management is provided for crowd energy and smart living. At the same time, a clear understanding is made for crowd energy concept and next generation smart living. Various case examples have been studied and a brief summary has been provided. Furthermore, a statistical analysis has been provided in terms of security management in smart living where it is found that young technocrats give the highest importance to security management in smart living. Last but not the least, current limitation, constraints, and future scope of security implementation have been discussed in terms of crowd energy clustered with next generation smart living.

Index Terms—Crowd energy, security management, smart living, statistical analysis.

1. Introduction

The industrial development of the world has raised the prosperity of life of at the cost of exhausting limited natural resources and damaging the environment. The consumption of fossil fuels, on which the industrial development has been largely based, has been recognized as a major cause of climate change. The impacts on the global ecosystem resulting from climate change are in turn expected to lead to substantial economic losses. Moreover, the global pollution due to traditional sources of energy moves scientists to search for other sources of green energy and to create a common platform for both energy producer and consumer. Our nation's electric power infrastructure known as "the grid" is rapidly reaching to its limit. We may get the electricity supply but the risks associated with that depending on the traditional structure are increased with the rising demand of the grid. So it is very essential to decentralize the entire power system to make it more secure and sustainable.

*Corresponding author
Manuscript received 2018-07-16; revised 2018-10-03.
M. S. A. Khan, M. A. R. Miah, and S. R. Rahman are with the Department of Electrical and Electronic Engineering, University of Asia Pacific, Dhaka 1205, Bangladesh (e-mail: DrShahrukh@ieee.org).
M. M. Iqbal is with Technical University of Munich, Munich, D-80333, Germany.
A. Iqbal is with the Department of Computer Science and Engineering, Chittagong Independent University, Chittagong, Bangladesh.
C. Aravind is with Taylor's University, Subang Jaya 47500, Malaysia.
C. K. Huat is with Universiti Tunku Abdul Rahman, Kampar 31900, Malaysia.
Publishing editor: Xin Huang

Smart living is altogether a new concept where technology adopts into day-to-day life to provide a comfortable, safer, convenient, and sustainable environment. Gradually, many countries around the world are trying to adopt the concept of smart living and related technology. Basically smart living is an idea which integrates technology with humanity. Smart living brings technology to all phases of human life necessity like food, housing, health, medication, education, transportation, and entertainment. The smart technology allows people to achieve smart living into all sectors of daily life and therefore a better world for upcoming generations. This paper brings out the new concept of crowd energy clustered into next generation smart living. This has been a complete new theory which is still under observation and indeed a very promising and emerging concept. But a very little study has been conducted in this short period of time. This paper finds the gap and tries to give a clear understanding of what crowd energy and smart living are as well as provides an analytical discussion on security management for both the emerging concepts.

2. Crowd Energy

Crowd energy is the combined effort of individuals or profit or non-profit organizations, or both, pooling their resources through online information and communications technology applications (ICT-applications) to help to implement the energy turnaround. It holds the concept of decentralization (production, storage, and consumption of renewable electricity) and a considerable change in society, economy, and politics[1]. According to [2], ICT will play an essential role in future power grids.

In addition to the crowd energy concept, the bidirectional flow of power between the grid and other consumers through a reliable and well-secured communications network is essential. A system controller will ensure a bidirectional interaction (cyber and physical) between the utility-side and the customer-side. This unit should be distributed, overseeing the local dispatch of energy in a way to optimize system reliability, quality, and the real-time trading of electricity. Moreover, a consumer can be turned into a producer whenever he supplies the electric energy produced in excess to his requirement. Intelligent generation storage load (iGSL) cells are the primary elements of the crowd energy concept. Introducing many cells in a network, connecting them by bidirectional communications lines, and finally processing the information in a crowd management system, yield to iGSL cells crowd. One issue is that the structure of the crowd does not have to be fixed. It is rather can be stated that the iGSL cells can and should vary over time.

Crowd energy system should be a socio-technological system. The mutual dependency between grid development and changing roles of end users must be considered. The iGSL cells make an energy consumer to become an energy producer. On the other hand, the prosumer is a new player in the energy (electricity) market and the prosumer is one of the important factors within the crowd energy concept helping to implement the energy turnaround. Fig. 1 shows a connection between traditional generation units with the prosumers. Now it is necessary to focus on the socio-psychological part of the crowd energy management side. When “the end points of consumption of electricity” (the electricity consumers) get incorporated to produce and store energy (electricity), they should have share their own electricity to the others after fulfilling their own demand. But why should they share? Motivations are required for the consumer to becoming a producer to share his own electric energy. The fields of human motivations are categorized into intrinsic and extrinsic ones. As Fig. 2 shows[3], the set of measures is directed to influence the intrinsic and extrinsic motivations of consumers to deploy renewables and smart grid technology (SGTs), participate in crowd energy, improve efficiency and reliability in an energy system, as well as increase public awareness and positive feedback[4],[5]. At the same time the policy maker decision in the favor of crowd energy is necessary[6].

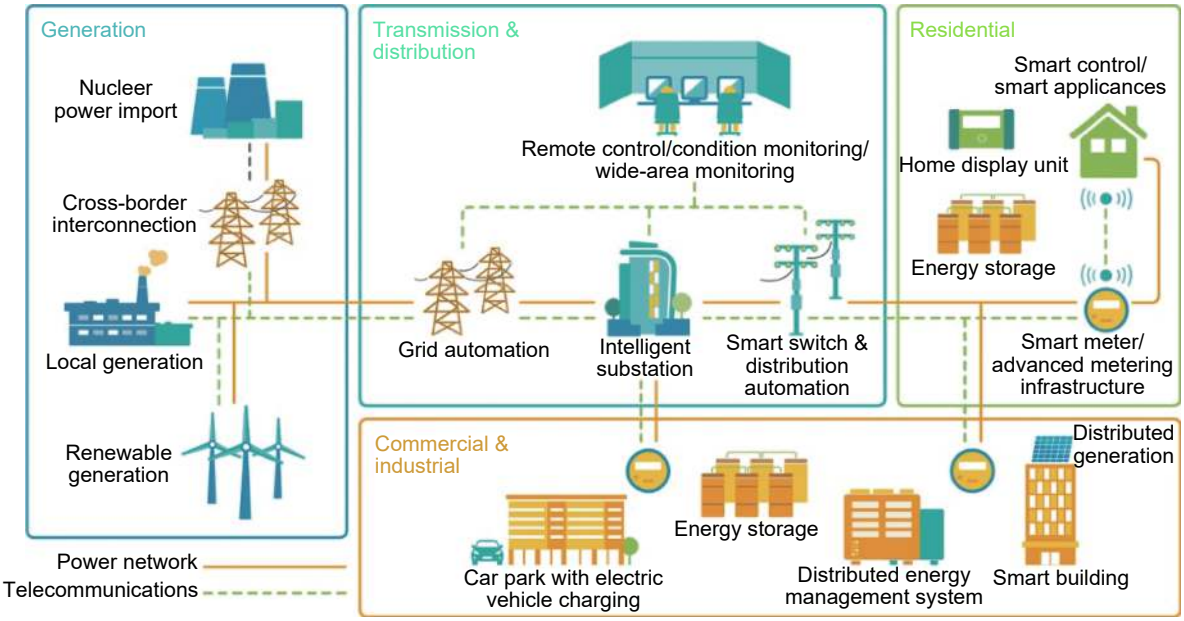

Fig. 1. Traditional generation unit and the prosumers are connected with a bidirectional communications line in the concept of crowd energy.

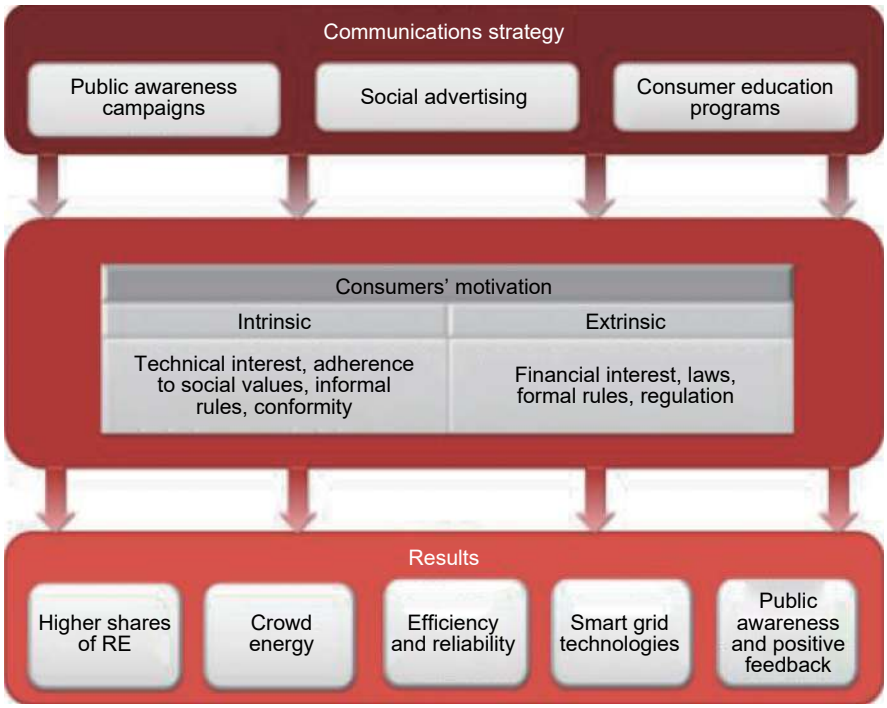

Fig. 2. Expected impact of the implementation of the communications strategy[3].

3. Security Management in Crowd Energy

The generation, transmission, and distribution of energy are among the most vital prerequisites for the functioning of modern societies[7]. ICTs are used to monitor, control, and operate power generation plants and power distribution within electric power supply system[8]. Process control systems, e.g., supervisory control and data

acquisition systems (SCADA systems), and other ICT systems used within electric power supply systems, are vulnerable to a multitude of physical, electromagnetic, and logical threats, both natural and man-made[9]. The recent trends are towards more general purpose software solutions; and towards the use of the Internet for communications related to operations and management of remote processes and production systems. The security issue should be maintained in crowd energy conception. A power system with crowd energy conception is a very complex network which contains millions of devices and whole components are connected with each other. So the security issue is a big concern for this huge network.

Crowd energy provides electricity demand from the centralized and distributed generation stations to the customers through transmission and distribution systems. The grid is operated, controlled, and monitored by using ICTs. These technologies deliver the power in an efficient way to the customers at a reduced cost. Crowd energy conception is based on two-way communications between prosumers and electric power generation and distribution companies. The two-way digital communications ensure the proper electricity consumption. Security system should be much reliable so that the communications channel works properly. Three main security objectives must be considered in the crowd energy system: 1) availability of uninterrupted power supply according to user demands, 2) integrity of communicated information between the prosumers and entity, and 3) confidentiality of user's data and the assurance of system safety.

Crowd energy network is a complex formation of different types of equipment which makes the system more vulnerable compared to the conventional power system network. These vulnerabilities might allow attackers to access the network, break the confidentiality and integrity of the transmitted data, and make the service unavailable. The following two vulnerabilities are the most serious in the crowd energy network:

■ Unorganized and weak communications between utility and prosumers might cause a lot of bad decisions, which creates too much vulnerability.

■ Having many stakeholders might give rise to a very dangerous kind of insider attacks which can create major damages.

And the followings are the recommendations to the vulnerabilities[10],[11]:

■ Ensure prosumers security when they are not in home.

■ Provide the security of several intelligent devices which are involved in managing both the electricity supply and network demand.

■ Physical security is needed for many components which are out of the utility's premises.

The attackers can cause a wide variety of attacks, which can be classified into three main categories[12],[13]: Component-wise, protocol-wise, and topology-wise. These three attacks can be further divided into different categories[14]-[17], such as:

1) Malware spreading;

2) Access through database links;

3) Compromising communications equipment;

4) Injecting false information;

5) Network unavailability;

6) Modbus security issue.

To prevent the attackers attack and to ensure the crowd energy network security, the following steps may be taken into consideration[18],[19]:

1) Strong authentication;

2) Mechanisms should be used to verify the prosumer identity;

3) Malware protection system should be incorporated in both the producer and consumer ends;

4) Network intrusion prevention system (IPS) and network intrusion detection system (IDS) technologies should augment the host-based defenses to protect the system from outside and inside attacks;

5) To ensure the security of the system, vulnerability assessments must be performed at least one in a year;

6) Awareness programs should be incorporated to educate the network users about the security of the system for using network tools and applications;

7) Control system and IT security engineers should be equally involved in securing with the crowd energy network;

8) Security issues must be considered as a part of the crowd energy design;

9) A robust authentication protocol is needed while communicating between the prosumers. Fig. 3 shows a security system model in crowd energy system.

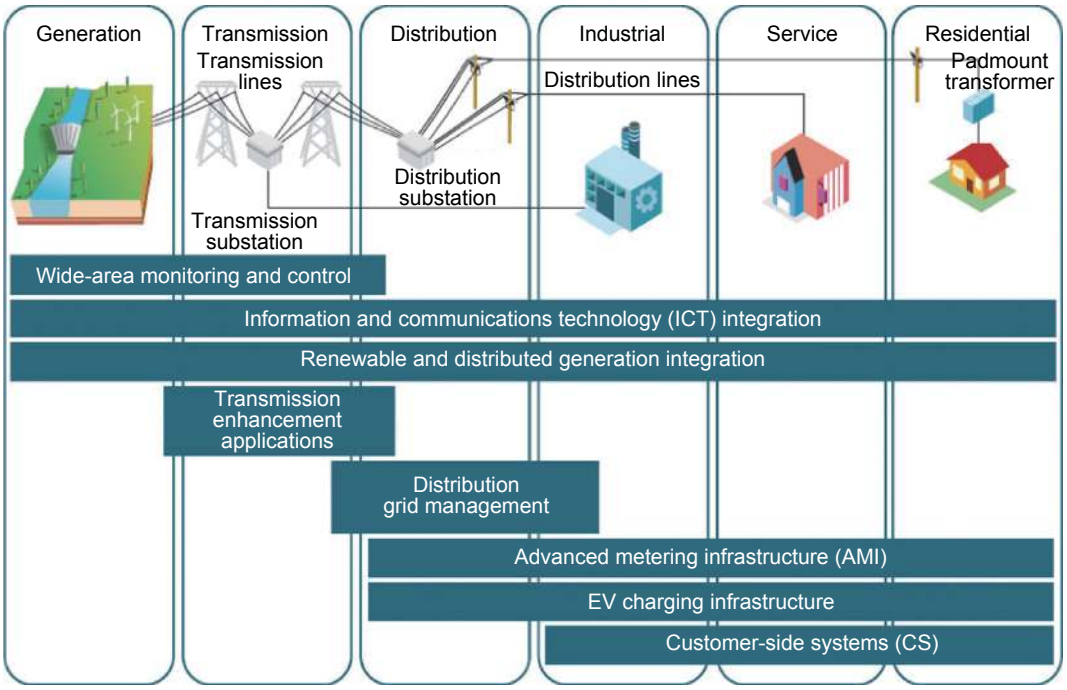

Fig. 3. Model security based design for crowd energy power system.

The following Section 4 describes the existing crowd energy models/systems so that the security layout of existing smart living technology can be found out, as shown in Fig. 4.

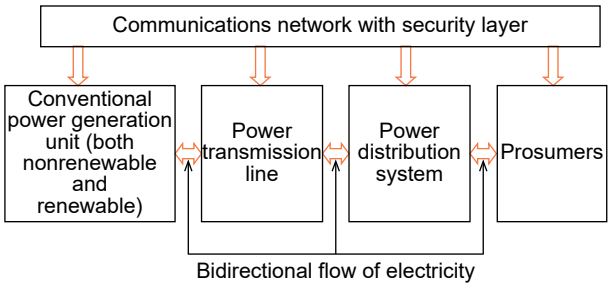

Fig. 4. Proposed security management model for crowd energy system.

4. Case Examples of Crowd Energy

According to [20], S. Abolhosseini *et al.* proposed that improving energy efficiency is an important way to reduce energy use and thereby CO_2 emissions, and to overcome the climate change problem. Energy efficiency for electricity networks can be considered in different stages, such as power generation, transmission, distribution, and consumption. For this purpose, thirty different energy efficiency technologies are available, including electric

vehicles, combined heat and power, virtual power plants, crowd energy, and smart grid. According to [21], R.-H. Zheng *et al*. considered one of the most prevalent ways to boost investment in renewable energy generation is to motivate individuals to participate into green energy investment and generation. However, not all individuals are willing or able to install on-site renewable energy generation at their homes. Therefore, a special crowd funding green energy investment has been recently introduced in the form of community shared renewable energy projects and it can be incorporated to crowd energy system.

5. Smart Living

Smart in general is a common term which refers knowledgeable, efficient, more controllable, adoptable, and sustainable. The definition of smart is different when it comes to technological advancements. J. Vasauskaite *et al*. precisely defined the term "smart" in [22] as according to them it mostly goes parallel to "intelligent". In addition, they mentioned five characteristics of "smart" which are adaptable, sensing, inferring, learning, and anticipating[22].

As renewables along with distributed smart grids, real time monitoring systems are being given importance constantly, the definition of "smart living" is changing every decade to further technological enhancements. Smart living is all about smart lighting, smart water, smart traffic, smart parking, smart building, smart industry, smart environment, location/context based service, and more. Smart living integrates all stakeholders such as people, machines, devices, and environment[23]-[25]. One of the major components of smart living is smart home. Smart home adapts smart designs and accommodates smart devices, intelligent technology, and sensors. But at present smart home means having efficient appliances and control devices to control lighting and temperature. Smart home design concepts also reflect the change in perception to adjust the needs of the environment and consumers, which can comprise of things such as regulations of room lighting and temperature and control of other machines and devices. The smart house would combine a number of smart communications systems which help residents to completely manage their own environment. To be precise, a smart home would be user-centric[25],[26].

In brief, smart home incorporates smart energy, smart mobility, digital healthcare, smart connectivity, smart shopping, home automation, smart comfort, and smart security.

6. Security Management in Smart Living

There is a word "stay smart, stay secure". Security management is a big issue in implementing smart living components. All the components are connected through various hardwares and softwares. A large number of devices, transmitting huge amount of data through many different APPs, are controlled through a secured management platform. Surge in data requires a new approach for speed, agility, and security. One of the technologies is being used extensively in smart living/smart house is Internet of things (IoT). But IoT has a high security issue in terms of data handling. Moreover, the configurations of some devices (sensors) are too weak to ensure protections. The hardware side or the device connectivity is not only guilty for this, but also the shortage of recognized security standards dedicated for the system. Fig. 5 shows a typical structure of security management system for smart living[27].

Security threats to smart home environments are existent and may be applicable to all devices and services. Sometimes the types of threats vary in different applications but they may cause significant damage in the overall structure and the environment may collapse. Thus, the following threats are still applicable such as physical attacks, unintentional damage, disasters/outage, damage/loss, and failure/malfunction.

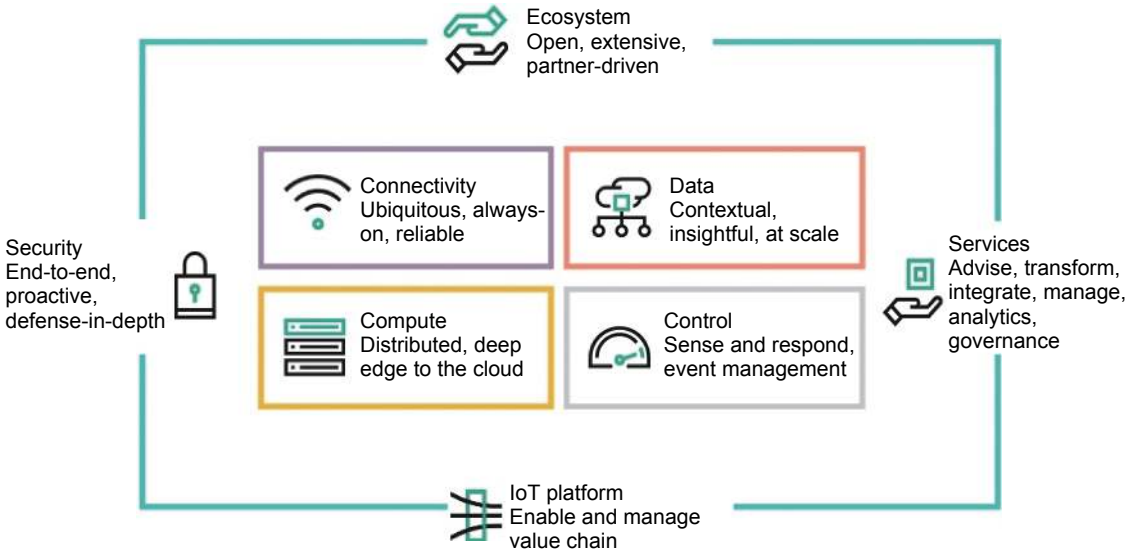

Fig. 5. Smart living security management[27].

Table 1 represents the concise interpretation of security concerns and defines which scenario disrupts security goals in the smart home[27],[28]. Therefore, security requirements, such as user and device authentication, monitoring the network integrity, availability, and confidentiality are desired. Fig. 6 might be a pathway to implementation of smart living addressing the security concerns. First of all, a plan should be carried out as an initialization of smart living. This includes the type of target consumer, project location, the environment, and more importantly the budget. The value proposition should be accounted carefully and express the result to the target consumer. Later, the project can be built to serve the target consumers as per their requirements and needs. After installation of the project components, test run should be processed to find out if there is any bug, security issues, customer concerns, etc. Finally, after the necessary optimization, the project may continue for a longer period of time.

Table 1: Smart home security challenges[28]

Scenario	Threats	Security goals
1	Message modification, eavesdropping message, customer data leakage	Confidentiality, authentication and integrity
2	Tampering, malicious software, modification, updating	Authenticity, integration
3	DoS attacks, reply attacks, repudiation	Non repudiation, integration, authentication
4	Message modified, eavesdropping, reply attacks	Availability, integration, authorization

7. Case Examples of Smart Living

Smart living technologies are still facing a chasm due to some reasons: Value propositions are not yet clear; existing solutions do not meet client needs; existing solutions lack interoperability, data security is not fixed; and there are too few live examples. There are some smart living projects ongoing around the world. T-city of Germany and Panasonic eco idea house and aware home at Georgia represent these projects. Fujisawa sustainable smart town (Tokyo, Japan) brings smart living to 1000 apartment residents[29]-[33].

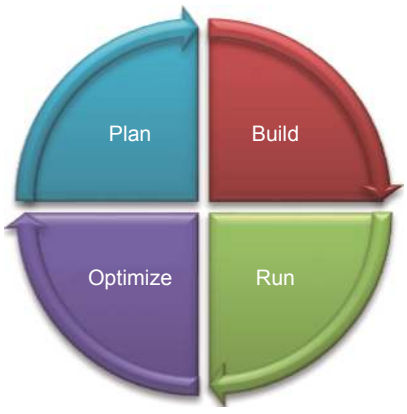

Fig. 6. Pathway for a sustainable smart living.

By creating a connected, sustainable, and comfortable living with innovative technology, the smart town offers solutions to energy management, security, assisted living, and mobility. In Adlershof (Berlin, Germany), 69 apartments, 29 studios, and 10 shops are practicing smart living with vision to create a real environment of self-determined future living at high comfort levels for everyone, to provide a live development, testing, and presentation platform with real user data, to develop key use cases and outcome technological challenges, and to drive public acceptance of smart home technology and connected life[23]. The above projections show that smart living technology concept has not merely been limited to cities (Germany), but also to schools (Georgia Tech.), and shops and enterprises (Panasonic). This shows that smart living technology is getting world's attention[33]-[35].

8. Statistical Analysis of Technical Know-How of Security Management among Technocrats

The survey was conducted by asking over two hundred respondents of different ages of technocrats, coming from engineering background. The survey portrays the smart living importance on current generation technocrats, mostly coming from engineering background. In addition, the reflection of security importance in energy management on those technology friendly people also has been tried to find out. Fig. 7 shows the age range of participants on the survey where it is clearly seen that the young generation dominates. This was made intentionally as smart living and security management in smart energy is said to be the next generation technology.

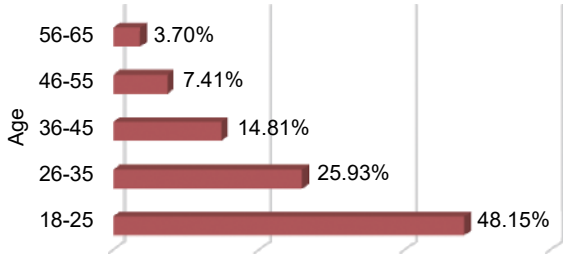

Fig. 7. Age range of the technocrats participated in the survey.

8.1. Question 1: How Important Is It to Have a Secure Supply of Oil, Gas, Coal, and/or Uranium?

Securing the supply of fossil fuels is one of the most crucial components of energy security. Fig. 8 reveals that this dimension is ranked at the top position by a majority of respondents. Interestingly, survey results revealed that people with different ages, gender, and levels of education prioritized the security of supply of primary energy resources. Almost 87 percent of the respondents feel it as a pure necessity.

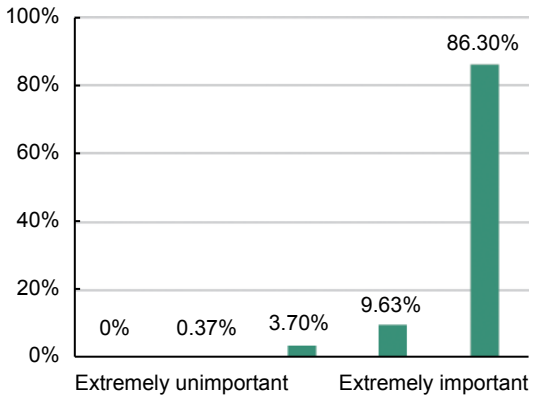

Fig. 8. Level of importance of securing supply of oil, gas, coal, and/or uranium.

8.2. Question 2: How Important Is It to Have Small-Scale, Decentralized Energy Systems?

For next generation smart security management, decentralized energy system (DES) plays one of the most important roles. Most of the security management needs to be implemented in the next generation, such as building to grid (B2G) and vehicle to grid (V2G) technologies which are the major parts of DES. Consequently, the smart renewables, including vertical axis wind turbines for low wind speed, low cost solar panels with smart sensors, real time smart monitoring for hybrid renewable interface, supercapacitor based switched control energy harvesting, and high data through multi-channel wavelength division multuiplexing (WDM) based optical fibre, are

being implemented for advanced living[36]-[39]. The need of DES in smart living has been reflected in Fig. 9. As a sign of favor against decentralization and towards large-scale, capital intensive infrastructure, Fig. 9 shows that how this dimension differed among respondents. Although around 66 percent respondents thought that it is important to have decentralized and small scale energy systems for energy security, around 33 percent respondents opined oppositely. It reflects the growing recognition about small scale renewable systems.

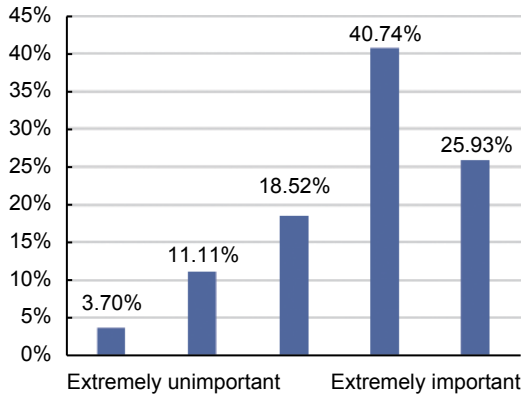

Fig. 9. Level of importance of having small-scale, decentralized energy systems.

8.3. How Important Is It to Conduct Research and Development on New and Innovative Energy Technologies?

Lastly, questions have been asked relating to the importance of encrypted security in smart home energy management system (SHEMS). Fig. 10 illustrates that almost 85 percent of the respondents gave above average importance to security management on new and innovative energy technologies. The respondents, giving it the highest importance, were mainly the people with post-graduation degrees.

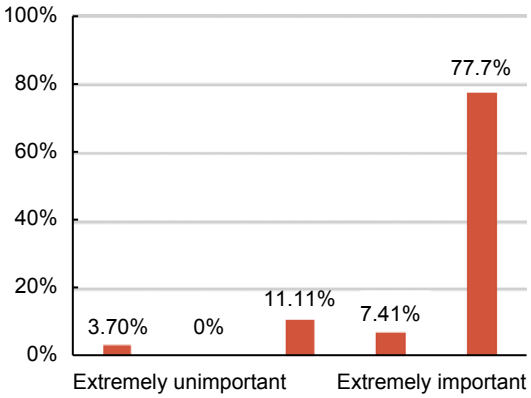

Fig. 10. Level of important about encrypted security in SHEMS.

9. Conclusion: Summary, Limitation and Future Scope

To summarize, it is not too much to say that the crowd energy concept is still a new theory and yet to be implemented in practical cases. The smart city living is surely the next generation planning and the current world is running with great pace at it. With the increase in renewables and breakdown in energy distribution, it is not too late to see a great smart-technological advance in this sector. The security management will definitely play a key-factor in the bidirectional flow of crowd energy clustered into next generation smart city living.

In conclusion, it was found that in terms of availability, the security of primary energy sources was amongst the most important dimensions. Although the rise of micro-grid and small scale renewable energy system is evident, decentralization was not as important to the respondents as security of supply. Young generation from Bangladesh with higher degrees from engineering level is giving security management to its utmost importance.

Acknowledgment

The authors would like to thank the support provided by the University of Asia Pacific and Institute for Energy, Environment, Research and Development (IEERD).

References

[1] S. Teufel and B. Teufel, “The crowd energy concept,” *Journal of Electronic Science and Technology of China*, vol. 12, no. 3, pp. 263-269, 2014.

[2] J. Wäfler and P. E. Heegaard, "A combined structural and dynamic modelling approach for dependability analysis in smart grid," in *Proc. of the 28th Annual ACM Symposium on Applied Computing*, Coimbra, 2013, pp. 660-665.

[3] V. Vereshchagina, M. Gstrein, and B. Teufel, "Analysis of the stakeholder engagement in the deployment of renewables and smart grid technologies," *Journal of Electronic Science and Technology*, vol. 13, no. 3, pp. 221-228, 2015.

[4] R. M. Ryan and E. L. Deci, "Intrinsic and extrinsic motivations: Classic definitions and new directions," *Contemporary Educational Psychology*, vol. 25, no. 1, pp. 54-67, Jan. 2000, DOI: 10.1006/ceps.1999.1020

[5] O. Çınar, Ç. Bektas, and I. Aslan, "A motivation study on the effectiveness of intrinsic and extrinsic factors," *Economics and Management*, vol. 16, no. 4, pp. 690-695, 2011.

[6] M. Gstrein and S. Teufel, "The changing decision patterns of the consumer in a decentralized smart grid," in *Proc. of the 11th Intl. Conf. on the European Energy Market*, Krakow, 2014, pp. 1-5.

[7] S. Antonsen, *Safety Culture: Theory, Method and Improvement*, Farnham: Ashgate, 2009.

[8] S. C. Patel and P. Sanyal, "Securing SCADA systems," *Information Management & Computer Security*, vol. 16, no. 4, pp. 398-414, 2008.

[9] S. K. Rodal. (2001). Sårbarhet I kraftforsyningens drifts-og styringssystemer. [Online]. Available: http://rapporter.ffi.no/rapporter/2001/04278.pdf

[10] I. L. G. Pearson, "Smart grid cyber security for Europe," *Energy Policy*, vol. 39, no. 9, pp. 5211-5218, Sept. 2011.

[11] S. Clements and H. Kirkham, "Cyber-security considerations for the smart grid," in *Proc. of IEEE PES General Meeting*, Providence, 2010, pp. 1-5.

[12] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde, "Protecting smart grid automation systems against cyberattacks," *IEEE Trans. on Smart Grid*, vol. 2, no. 4, pp. 782-795, Dec. 2011, DOI: 10.1109/TSG.2011.2159999

[13] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An integrated security system of protecting smart grid against cyber attacks," in *Proc. of Innovative Smart Grid Technologies*, Gothenburg, 2011, pp. 1-7.

[14] V. Aravinthan, V. Namboodiri, S. Sunku, and W. Jewell, "Wireless AMI application and security for controlled home area networks," in *Proc. of IEEE Power and Energy Society General Meeting*, Detroit, 2011, pp. 1-8.

[15] Y. L. Mo, T. H. J. Kim, K. Brancik, *et al*., "Cyber-physical security of a smart grid infrastructure," *Proc. of IEEE*, vol. 100, no. 1, pp. 195-209, Jan. 2012, DOI: 10.1109/JPROC.2011.2161428

[16] B. Flynn. (June 2008). Wireless smart grid security. *Cyber Security for Process Control Systems Summer School*. [Online]. Available: https://tcipg.org/cyber-security-process-control-systems-summer-school-2008

[17] X.-D. Wang and P. Yi, "Security framework for wireless communications in smart distribution grid," *IEEE Trans. on Smart Grid*, vol. 2, no. 4, pp. 809-818, Dec. 2011, DOI: 10.1109/TSG.2011.2167354

[18] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Trans. on Smart Grid*, vol. 1, no. 1, pp. 99-107, Jun. 2010, DOI: 10.1109/TSG.2010.2046347

[19] S. Iyer, "Cyber security for smart grid, cryptography, and privacy," *Intl. Journal of Digital Multimedia Broadcasting*, vol. 2011, pp. 372020:1-8, Jul. 2011.

[20] S. Abolhosseini, A. Heshmati, and J. Altmann. (2014). A review of renewable energy supply and e nergy efficiency technologies. *Social Science Electronic Publishing*. [Online]. Available: https://www.researchgate.net/profile/Osama_Suleiman/project/exploitation-of-renewable-energy-in-sudan/attachment/57f110a608aeb9635636dfda/AS:412739735441409@1475416229962/download/dp8145.pdf

[21] R.-H. Zheng, Y. Xu, N. Chakraborty, and K. Sycara, "A crowd funding model for green energy investment," in *Proc. of the 24th Intl. Conf. on Artificial Intelligence*, Buenos Aires, 2015, pp. 2669-2675.

[22] J. Vasauskaite, S. Teufel, and B. Teufel, "Smart framework: Application under the conditions of modern economy," *Inzinerine Ekonomika-Engineering Economics*, vol. 28, no. 2, pp. 180-186, 2017.

[23] C. P. Liyanage and A. Marasinghe, "Planning smart meal in a smart city for a smart living," in *Proc. of Intl. Conf. on Biometrics and Kansei Engineering*, Tokyo, 2013, pp. 166-171.

[24] M. S. A. Khan, R. K. Rajkumar, C. Aravind, Y. W. Wong, and M. I. F. Bin Romli, "A LabVIEW-based real-time GUI for switched controlled energy harvesting circuit for low voltage application," *IETE Journal of Research*, 2018, DOI: 10.1080/03772063.2018.1510747

[25] M. S. A. Khan, R. K. Rajkumar, C. Aravind, and Y. W. Wong, "A novel approach towards introducing supercapacitor based battery charging circuit for off-grid low voltage maglev VAWT," *Intl. Journal of Control Theory and Application*, vol. 9, no. 5, pp. 369-375, 2016.

[26] M. S. A. Khan, R. K. Rajkumar, and C. Aravind, "Optimization of multi-pole three phase permanent magnet synchronous generator for low speed vertical axis wind turbine," *Applied Mechanics and Materials*, vol. 446-447, pp. 704-708, Nov. 2013.

[27] W. Ali, G. Dustgeer, M. Awais, and M. A. Shah, "IoT based smart home: Security challenges, security requirements and solutions," in *Proc. of the 23rd Intl. Conf. on Automation and Computing*, Huddersfield, 2017, pp. 1-6.

[28] B. C. Doepfer. Smart living@home—-insights, technologies, and user centric solutions from fujisawa and future lining Berlin. [Online]. Available: https://www.slideshare.net/M2M_Alliance/smart-living-home

[29] C. K. Lee, J. Lee, P. W. Lo, *et al*., "Taiwan perspective: Developing smart living technology," *Intl. Journal of Automation and Smart Technology*, vol. 1, no. 1, pp. 93-106, 2011, DOI: 10.5875/ausmt.v1i1.74

[30] F. S. Ferraz and C. A. G. Ferraz, "Smart city security issues: Depicting information security issues in the role of an urban environment," in *Proc. of the IEEE/ACM 7th Intl. Conf. on Utility and Cloud Computing*, London, 2014, pp. 842-847.

[31] J. Bugeja, A. Jacobsson, and P. Davidsson, "On privacy and security challenges in smart connected homes," in *Proc. of European Intelligence and Security Informatics Conf.*, Uppsala, 2016, pp. 172-175.

[32] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, "Security and privacy issues for an IoT based smart home," in *Proc. of the 40th Intl. Convention on Information and Communication Technology, Electronics and Microelectronics*, Opatija, 2017, pp. 1292-1297.

[33] S. Yoon, H. Park, and H. S. Yoo, "Security issues on smarthome in IoT environment," in *Computer Science and its Applications: Ubiquitous Information Technologies*, J. J. Park, I. Stojmenovic, H. Y. Jeong, and G. M. Yi, Eds. Berlin, Heidelberg: Springer, 2015.

[34] E. Zeng, S. Mare, and F. Roesner, "End user security & privacy concerns with smart homes," in *Proc. of the 13th Symposium on Usable Privacy and Security*, Santa Clara, 2017, pp. 65-80.

[35] European Union Agency for Network and Information Security. Security and resilience of smart home environments. [Online]. Available: https://www.enisa.europa.eu/publications/security-resilience-good-practices

[36] M. S. A. Khan, R. K. Rajkumar, C. Aravind, and Y. W. Wong, "Comprehensive review of the wind energy technology," *Intl. Journal of Control Theory and Applications*, vol. 9, pp. 2819-2816, 2016.

[37] M. S. A. Khan, R. K. Rajkumar, Y. W. Wong, and C. A. Vaithilingam, "Feasibility study of a novel 6V supercapacitor based energy harvesting circuit integrated with vertical axis wind turbine for low wind areas," *Intl. Journal of Renewable Energy Research*, vol. 6, no. 3, pp. 1167-1177, 2016.

[38] M. S. A. Khan, "Instantaneous charging & discharging cycle analysis of a novel supercapacitor based energy harvesting circuit," in *Proc. of the 3rd Intl. Conf. on Mechanical Engineering and Automation Science*, 2017, pp. 020046:1-8.

[39] M. S. A. Khan, M. Howlader, and M. A. R. Miah, "Performance analysis of receiver power sensitivity of advanced modulation formats in WDM based standard mode fibre for next generation data rate," in *Proc. of the 4th Intl. Conf. on Advances in Electrical Engineering*, Bangladesh, 2017, pp. 395-399.

MD Shahrukh Adnan Khan has an all through first class academic career in his life. He obtained his Ph.D. degree from University of Nottingham, Semenyih, Malaysia in 2011 with an outstanding record-breaking result. He achieved the Member of the Institution of Engineering and Technology (MIET) certificate from Institution of Engineering and Technology (IET), Stevenage, UK in 2018. Currently, he is an assistant professor at University of Asia Pacific (UAP), Dhaka, Bangladesh. His current interest lies in energy storage, renewable energy, electrical machines, smart living, real time control system, optical fiber, advance modulation techniques, and environmental science. He has over 50 publications in high quality peer reviewed journals and conferences. Furthermore, He is an IEEE Young Professional and Life-Fellow in Notre Dame Alumni Association & Nottingham Alumni Association.

Muhammad Ahad Rahman Miah is currently working as an assistant professor with the Department of Electrical and Electronic Engineering, University of Asia Pacific. He was awarded Her Majesty the Queen Scholarship of Thailand for his graduate studies at Asian Institute of Technology (AIT), Bangkok, Thailand. His research interests include power systems, smart grid, renewable energy, energy conversion and management, and energy auditing.

Shaikh Rashedur Rahman received his M.Sc. degree in electrical and electronic engineering from Islamic University of Technology (IUT), Dhaka, Bangladesh in 2016. He received his B.Sc. degree (Honors) (Securing First Position) from UAP in 2012. He was awarded the Chancellor's Gold Medal for securing the highest distinctions among all departments in undergraduate studies in his B.Sc. degree. Currently, he is working as an assistant professor with the Department of Electrical and Electronic Engineering, UAP. His research interests include power system, renewable energy, digital electronics, and solid state device. He has several publications in different international journals and conferences.

Mirza Mursalin Iqbal received his M.Sc. degree in power engineering from Technical University of Munichin, Munich, Germany in 2015. He completed his B.Sc. degree (Honors) (Securing Fifth Position) from IUT in 2010. He is now working as an assistant professor with the Department of Electrical and Electronic Engineering, UAP. His research interests include renewable energy sources, power systems, power system protection, and power electronics. He has published several research papers in different international journals.

Aseef Iqbal received his Ph.D. degree in mechatronics, robotics, and automation engineering from Universiti Islam Antarabangsa Malaysia, Selangor, Malaysia in 2015. He is currently serving as an assistant professor at Chittagong Independent University, Chittagong, Bangladesh with a demonstrated history of working in the higher education industry. He is skilled in human-robot interaction, mechatronics, computer vision, artificial intelligence, and mobile robotics.

Aravind CV received his Ph.D. degree from Universiti Putra Malaysia, Serdang, Malaysia in 2013. He is currently the programme director of electrical and electronic engineering at Taylor's University, Subang Jaya, Malaysia. His research interests include electrical machine design for wind energy generators and for electric vehicles.

Chua Kein Huat was born in Malaysia in 1979. He is currently working as an assistant professor with the Department of Electrical and Electronic Engineering at Universiti Tunku Abdul Rahman (UTAR), Kampar, Malaysia. He received his B.Eng. degree in electrical, electronic and systems from Universiti Kebangsaan Malaysia, Bangi, Malaysia in 2004, the M.Eng. degree in electrical energy and power system from University of Malaya, Kuala Lumpur, Malaysia in 2009, and the Ph.D. degree in electrical engineering from UTAR in 2016. His research areas focus on the applications of energy storage system, energy management system, power protection system, and fuzzy logic control. He is also a Registered Electrical Energy Manager (REEM) with Energy Commission Malaysia.