International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 4, August 2020, pp. 3978~3987
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i4.pp3978-3987

Advanced energy management system with the incorporation of novel security features

Raheel Muzzammel, Rabia Arshad, Saba Mehmood, Danista Khan
Department of Electrical Engineering, University of Lahore, Pakistan

Article Info

Article history:

Received Nov 14, 2019
Revised Mar 5, 2020
Accepted Mar 16, 2020

Keywords:

Energy management system
Energy theft detection
Message digest-5 algorithm
Reduction of CO_2 emission
Renewable energy sources

ABSTRACT

Nowadays, energy management is a subject of great importance and complexity. Pakistan, being in a state of developing country, generates electrical power mainly by using non-renewable sources of energy. Non-renewable entities are fossil fuels such as furnace oil, natural gas, coal, and nuclear power. Pakistan has been facing a severe shortage of production in energy sector for last two decades. This shortfall is affecting the industrial development as well as economic growth. With the growing population, the load demand is rapidly increasing and there must be a need to expand the existing ones or to build new power systems. In this paper, an autonomous management system has been proposed to enhance quality, reliability and confidence of utilization of energy between end consumers and suppliers. Such objectives can only be fulfilled by making the power supply secure for end consumers. Distributed and centralized control systems are involved for maintaining a balance between renewable energy resources and base power, so that end consumers demand can be fulfilled when required. A reliable Two-way communication system between suppliers and end consumers has been proposed by using Message Digest algorithm which ensures that there would be no energy theft. Simulations have been done in MATLAB/Simulink environment and results have been presented to show the effectiveness of proposed model.

Corresponding Author:

Raheel Muzzammel,
Department of Electrical Engineering,
University of Lahore, Pakistan.
Email: raheel.muzzammel@ee.uol.edu.pk

1. INTRODUCTION

Role of electrical power is an essential part towards enhanced industrial growth and to raise living standard of general public. According to water and power development authority (WAPDA), government has to spend about billions of US dollars per year to import oil to meet requirements of an electricity supply companies in Pakistan. Energy crises need a prompt action and it should be addressed within next decades. To do this, one must switch towards renewable energy sources and to minimize usage of non-renewable sources.

A lot of research has been conducted to increase practical impact of renewable energy sources. Wind energy conversion system (WECS) is developed in optimal power flow (OPF) model [1]. Weibull distribution is utilized to determine optimal wind speed for generation and distribution of power in a stochastic way [2-4]. For storing excess energy, a battery is added which can be retrieved at night or when sunlight is obstructed. For battery protection from overcharging, a charge controller is used [5].

With introduction of renewable energy technology at consumer end, geography of power system is totally changed. Consumers have ability to produce energy for utilization. Concept of two-way flow of power is matured. Therefore, there is an immediate need to devise improvements in energy management system (EMS). A highly secured and enabled communication between end consumer and supplier is established. Encryption

and decryption of information is done for enhancing the security [6, 7]. An autonomous management system is made in the researches to enhance the quality of utilization of energy between consumers and suppliers [8-12].

Theft detection is done by measuring power on both sides; load and distribution transformer. Imposters use different techniques to steal. Therefore, different techniques for theft detection must be developed to overcome such events of energy theft. [7, 13]. Blowfish, advanced encryption standard (AES), data encryption standard (DES) and Triple Data Encryption Standard (3DES) are common symmetric algorithms. It is found from literature that Blowfish is the best in terms of encryption time, decryption time, memory usage, power consumption, latency, and jitter and security level. On the other hand, rivest shamir adleman (RSA), elliptic curve cryptography (ECC) and Ellamae are the common asymmetric algorithms. It is found from literature that ECC is best in almost all parameters except in signature verification time. Secure hashing algorithm (SHA1) and (SHA256) are also found in research but because of its increase encryption time on large input size and more power consumption, it is impractical to implement [14, 15]. In this research, message digest (MD5) algorithm is implemented for securing communication between supplier and consumer because of its less encryption time and power consumption [12, 14-18].

It is possible to maintain power production system with carbon dioxide emission reaching to zero with help of incorporation of renewable energy resources. Reduction in CO_2 emission is being considered in all other developed countries like India, Romania, Germany, UK and Denmark; Germany and Denmark. That's why it should be considered by developing countries like Pakistan as well. Wind power generation is found to be the best renewable energy source for energy generation in India so that India is focusing on wind power generation and is successful in easily elimination of effects of global warming [19, 20]. Renewable energy sources can be integrated with the conventional grids through high voltage direct current transmission (HVDC) via maximum efficiency and transferability [21-25].

In this research, renewable energy sources-based EMS is developed and further, security features are incorporated to cease cyber-attacks and energy theft. Hardware prototype is developed for EMS. Simulations are carried out in MATLAB/Simulink. Rest of paper is designed in following sections. Comprehensive details about message digest algorithm for security is covered in section 2. Section 3 contains the details about proposed methodology of this research. Section 4 covers hardware model. Results and simulations has been presented in section 5. Scope of commercialization of the proposed idea is given in section 6. Sections 7 and 8 consist of possible future directions that can be incorporated in this research and conclusion of this research work respectively.

2. SECURITY ALGORITHM FOR ENERGY MANAGEMENT SYSTEM (EMS)

2.1. Message digest algorithm

Message digest (MD), also known as Hash algorithm, generates a sole digested message for any message. Hash function is a kernel of MD algorithm which abridges a string of any length to string for a fixed length. Hash password encryption (HPE) is an approach of encryption used for MD5. MD5 algorithm has irreversible and non-counterfeit feature. Therefore, MD5 algorithm is more superior in its anti-tamper capability. This research implements a data integrity checking system based on MD5 algorithm as shown in Figure 1.

2.1.1. Steps to implement MD5 algorithm

Message-digest algorithm (MD5) flowchart is described in the following steps:

a. First check the length of number of bits of the original message.
b. To bring about the input message multiple of 512-64 (the add bits: 1 0 0 .....0), add the number of bits to input message.
c. Now, add the 64-bits that indicates the length of input message to result of the 2ndpoint, final result will be denoted by "M" (Multiple of 512-bits).
d. "M" is divided to the blocks (B), in which each of them is of 512 bits.
e. "B" is further divided into 16 blocks (X), in which each one includes 32-bits.
f. This algorithm consists of 4 rounds, each round contains 16 steps. So, by this there are total 64 steps.
g. There are four 32-bit shift registers, all shift registers have some initial values (Hex.) as given in the following:

$$\text{Register A} = [6\ 7\ 4\ 5\ 2\ 3\ 0\ 1]\ 32-\text{bits};\ [A] = [D]'$$

$$\text{Register B} = [e\ f\ c\ d\ a\ b\ 8\ 9]\ 32-\text{bits};\ [B] = [C]'$$

$$\text{Register C} = [9\ 8\ b\ a\ d\ c\ f\ e]\ 32-\text{bits};\ [C] = [B]'$$

$$\text{Register D} = [1\ 0\ 3\ 2\ 5\ 4\ 7\ 6]\ 32-\text{bits};\ [D] = [A]$$

h. The values of A, B, C and D are temporarily stored in AA, BB, CC, and DD respectively.
i. This is core of algorithm which has 4 rounds of processing. Every round involves 16 steps and every single step is using a "table" T of 64 elements [0....63], for T[i], where "i" is the index. Thus, the four rounds have the correspondent structure, but each uses mismatched functions name as F, G, H and I.

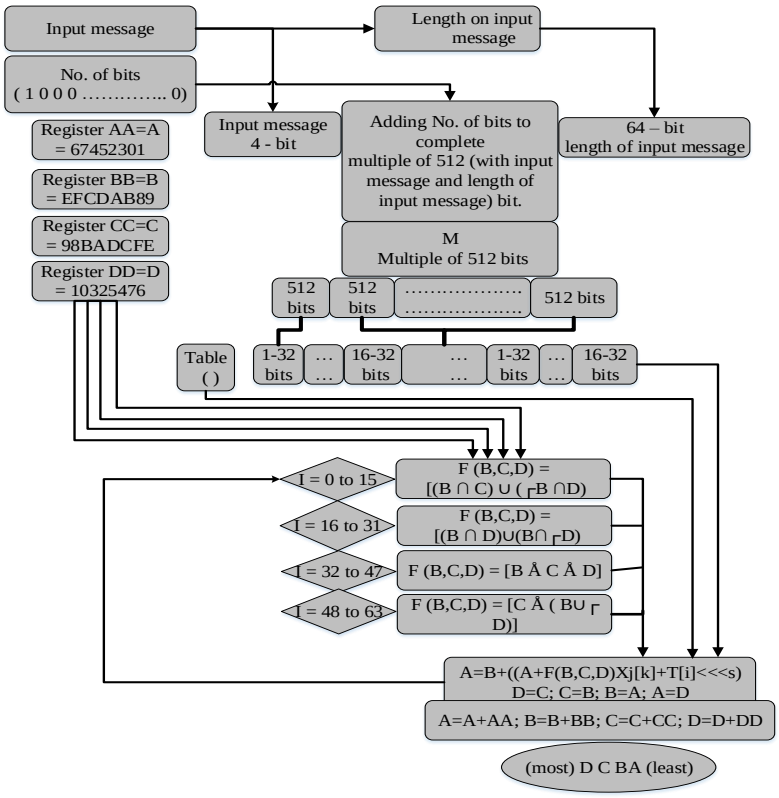


Figure 1. Message digest-5 algorithm flow chart

$$F(B, C, D) = [(B \wedge C) \vee (\neg B \wedge D)], T[0-15], \text{includes 16 steps}$$

$$G(B, C, D) = [(B \wedge D) \vee (B \wedge \neg D)], T[16-31], \text{includes16 steps}$$

$$H(B, C, D) = [B \oplus C \oplus D], T[32-47], \text{includes 16 steps}$$

$$I(B, C, D) = [C \oplus (B \vee \neg D)], T[48-63], \text{includes 16 steps}$$

where the symbols $\vee$ represents logical OR, $\wedge$ represents logical AND, $\neg$ represents logical NOT and $\oplus$ represents logical XOR. The operation in single step involves the functions:

$$A = B + ((A + F(B, C, D) + X_j[k] + T[i]) <<< s)$$

$$D = C; C = B; B = A; A = D$$

where $X_j[k] - k^{th}X$ (divided of B) and J[th] number of blocks (B-512 bits) and <<<s-circular shift left by s-bits. After four rounds, the output is added to input of the first round.

$$A = A + AA; B = B + BB; C = C + CC; D = D + DD$$

j. Then, the output is of 128-bits and will be ordered as follows:

$$(most)\boldsymbol{D} --> C --> B --> A\ (least)$$

3. METHODOLOGY

In this project, a clear energy generation is promoted by incorporation of renewable energy technologies. Proposed block diagram of this research project is shown in Figure 2(a). Data transferable security features are also introduced in this project by converting data in hash form with help of MD5 algorithm as shown in Figure 2(b).

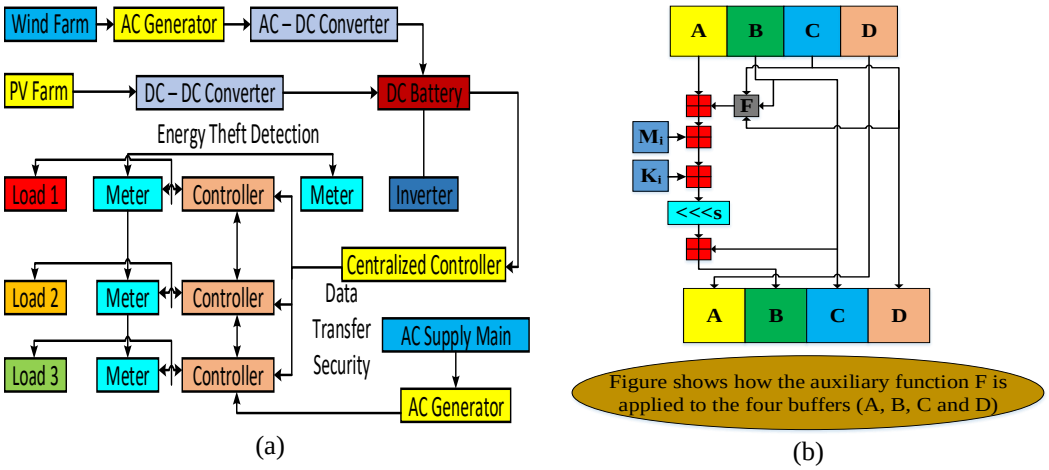


Figure 1. (a) Proposed model of energy management system, and (b) proposed encryption technique for data transfer security between consumer and supplier

4. HARDWARE DEVELOPMENT OF PROTOTYPE MODEL

Hardware prototype model is developed as shown in Figure 3 to increase the practicality and realization of proposed research.

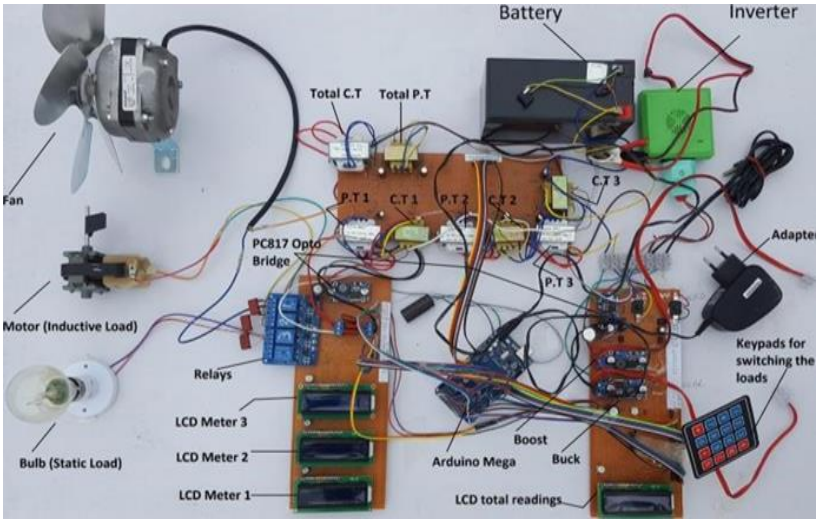


Figure 3. Hardware development of prototype/test model for validation of advanced energy management system and security features

5. SIMULATION RESULTS AND ANALYSIS

Proposed model is simulated on Matlab/Simulink and apparent power is analyzed as shown in Figure 4. This analysis helps in determining the operation of energy management system within prescribed limits for genrration and demand. Load demands with respect to generation from different sources are listed in Table 1.

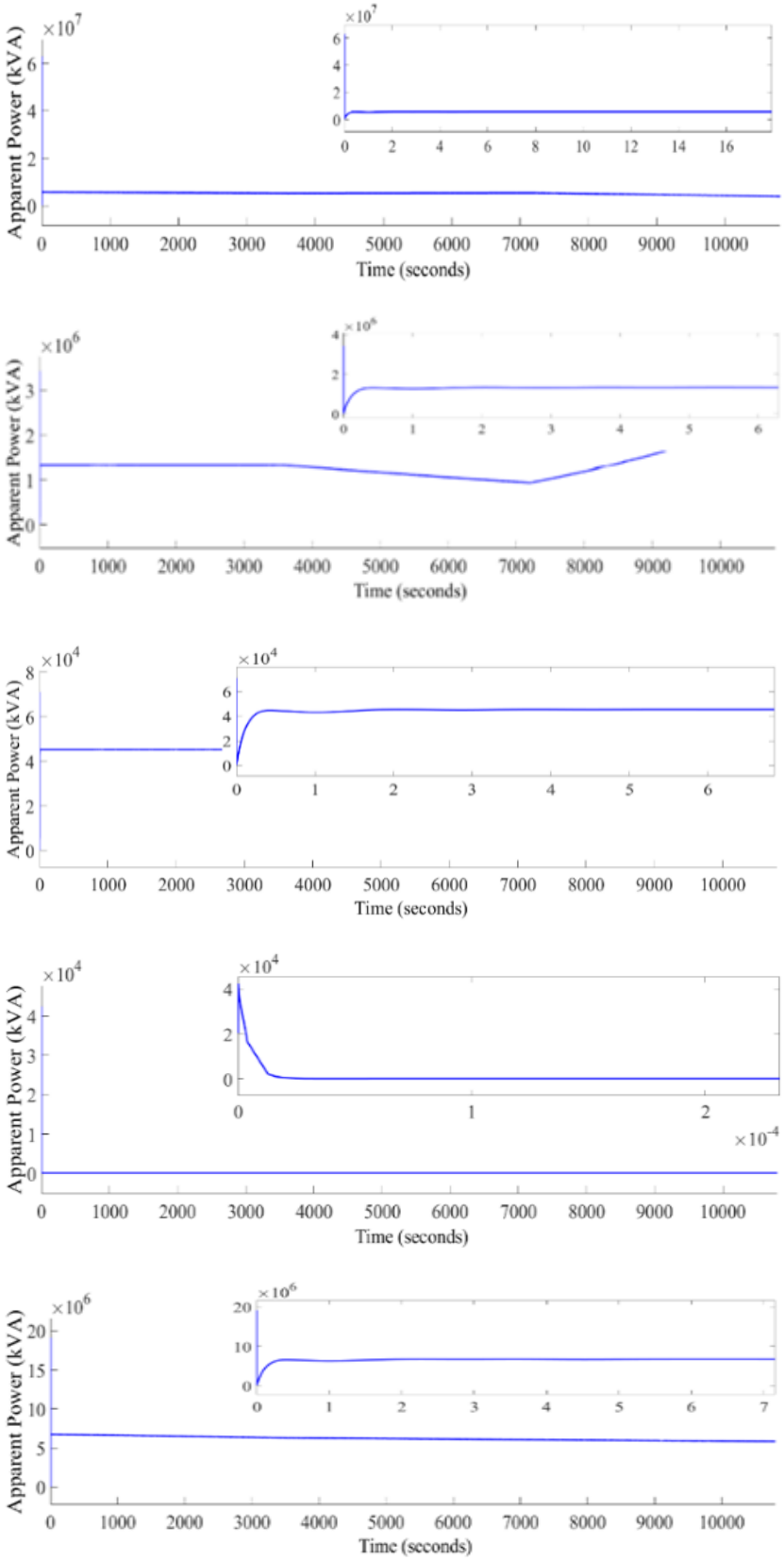


Figure 2. Characteristics of apparent power for analyzing operation of, (a) thermal generation, (b) wind power generation, (c) PV based generation, (d) industrial load, and (e) residential load

Table 1. Data of generation and demand

Parameters	Generation			Demand	
	Diesel Engine	PV Farm	Wind Farm	Industrial Load	Residential Load
V (V)	8353	188.4	8349	8348	8349
I (A)	480.3	4848	3.784	0.008351	561.7
S(kVA)	6.018e6	1.37e6	4.739e4	104.6	7.035e6
P (kW)	6.017e6	1.23e6	2.527e4	-104.6	-6.941e6
Q (kVAR)	8.692e4	-7.846e6	-4.009e4	-0.007682	1.146e6

5.1. Message digest algrithm results

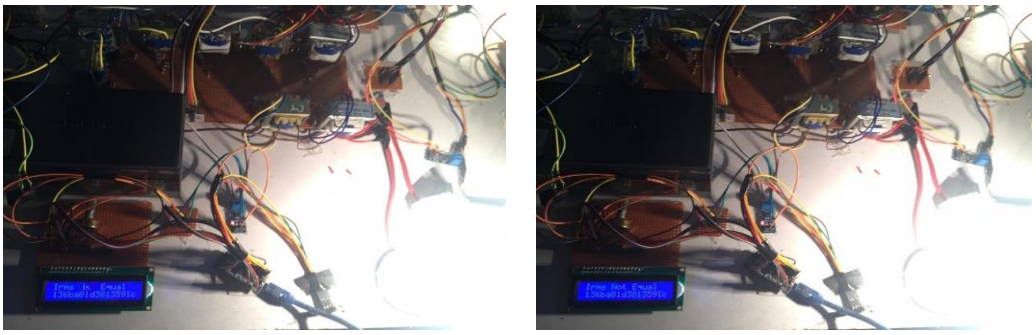
Message digest algorithm is implemented to secure the energy management system. Information about consumer parameters can be encrypted and then transferred to supply company to compare sending and receiving information. This will help against any cyber-attacks on the power networks and will also help in theft detection. For proposed model, currents I_{rms} both on the load as well as on the supply side are shown along with their hashed value. When there is no theft, the hashes are same on both sides and during theft, the hashes are seen to be different on both the sides as shown in Table 2 and Table 3 and in Figures 5 and 6.

Table 2. Hashed texts on load and supply side during no theft

Parameters	Currents	Hashed Texts
Supply	0.65 A	136ba81d3813591cdcc15fcb924b9437
Load	0.65 A	136ba81d3813591cdcc15fcb924b9437

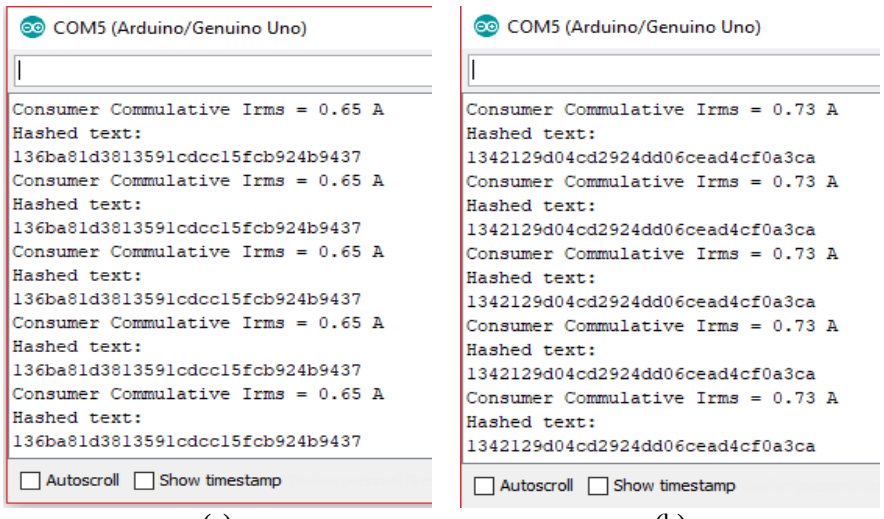
Table 3. Hashed texts on load and supply side during theft

Parameters	Currents	Hashed Texts
Supply	0.65 A	136ba81d3813591cdcc15fcb924b9437
Load	0.73 A	1342129d04cd2924dd06cead4cf0a3ca



(a) (b)

Figure 5. LCD screen during, (a) no theft, (b) theft



(a) (b)

Figure 6. (a) Similarity, and (b) difference of hashes of supply and consumer end

6. BUSINESS PLAN FOR COMMERCIALIZATION

6.1. Scope of commercialization

The proposed model highlights the importance of secured energy management with the incorporation of renewable energy technology. World is moving and discovering ways of generation of clean electricity. Supply companies are making consumers autonomous by allowing them to generate electricity by their own and sale as and when excess energy production is available. In this project, a prototype is prepared to demonstrate the importance of using renewable energy sources and secure communication between consumers and suppliers to avoid energy theft.

This project hits the small and medium sized production and manufacturing industries. Home based industries are also considered. Further, supply companies like faisalabad electric supply company (FESCO), lahore electric supply company (LESCO) etc., and consumers involved in the generation by renewable energy sources will be the most convincing customers of this idea. The companies which are serious about health safety and environment and are interested to obtain ISO certifications, can take interest in this prototype of idea. This project is successful providing a door to reduce CO_2 emissions.

Research and development involved in IOT can take interest to provide funds to commercialize the prototype with the facilities that are beyond limitations involved because of distance between consumer and appliances without any fear of cyber intruder. This project secures the wireless communication between consumer and supplier by considering the encryption through message digest algorithms and decryption via brute force attack. Therefore, this project is basically hitting the markets and investors involved and interested in interdisciplinary research and fields of ICT and Power sector.

6.2. Financial viability

Financial viability of this idea for small and medium scale industries and consumer sides at residential and commercial areas is very high. A little investment results in making systems intelligent and autonomous by securing communication with this idea. Further, reduction in CO_2 emission involves HSE and ISO certifications. Therefore, with the idea of moving towards generation via renewable resources, we cannot deny the energy management importance with the incorporation of renewable energy sources. Importance of energy management is also increased because of inflation and reduction in the capacity of acquiring capital because of decrease in the worth of rupee in Pakistan. Further, cost/benefit ratio is within acceptable limit for this idea. Rates of energy are very much independent of supply companies' tariffs with this idea.

6.3. Ease of development

Since a prototype is prepared in this project to analyze the performance of innovation, direct deployment is not possible. Changes are required with respect to the consumer's specifications. However, module required for encrypting and decrypting information transferred via wireless link can be deployed easily with a slight modification. Further, energy theft detection can be implemented without any alteration.

6.4. Scalability

As prototype is prepared, this project requires a scalability with respect to customer's properties. Further, quantitative vs qualitative evaluation is required to enhance the outcomes of this research project.

7. POSSIBLE FUTURE DIRECTIONS

Some of the ideas for future development is mentioned below:

a. Latest ways of encryption and decryption like Advanced Encryption Standard, Triple Data Encryption Standard, Twofish etc., will secure the communication between consumer and producers. This will help the consumer to act as prosumer. Prosumer is a category in which consumer has the ability to sale electricity to supply companies when excess generation is available at its side. Latest techniques of encryption and decryption will make consumer more autonomous without any fear of cyber-attack.
b. Features of smart meters can be added to introduce the concept of peak hours and off peak hours pricing. This will give birth to the concept of smart billing system for power facilities.
c. Calculation of thermal aging of components of power system will enable the supplier to intelligently handle the power transferring in the time of peak hours to avoid long term shut down in case of any cable or components failure. Temperature sensing and x-rays imaging will add fuel to this project for prolonging life.
d. Concept of two-way flow of power can be introduced and theft detection system can be upgraded according to this idea. Not only magnitude of current but also direction of flow of current can be used for theft detection.

e. IoT based configurations can be introduced in this project. Data of the current configuration of the system will be thrown over the cloud and can be accessed throughout the world with the private key. This will make the distance free app for automating energy management.

Intelligent robots can be integrated with this system to access to the points where automation is failed. These robots can be equipped with drones for landing to the faulty points or can be made travelled over the power lines like an electric cable car to the points of failures. This would help in activating timely remedial actions for manual operation of tripping faulty sections from the system.

8. CONCLUSION

Energy crises can be resolved in next decades using this advanced energy management system. This system provokes the maximum utilization of renewable energy sources along with a little reliance on conventional sources. Therefore, promotion of green energy and energy mix model is the main motivation existing behind this approach. Energy management system is simulated. Further, prototype of energy management system is developed to validate the idea of energy management with the incorporation of renewable energy sources and advanced security features. It is noticed from the recent trends of power generation that world is moving towards renewable energy sources for power production. It is because of many reasons. Some of the remarkable reasons are decrease in the fossil fuel energy reservoirs, global warming and excess CO_2 emissions. Therefore, world is looking for other sources of generation. It is found from the recent articles of energy that developed countries like England, Germany will move their entire system of power generation to renewable energy sources by the end of 2030.

Therefore, this research provides a brief introduction of energy management system with the ability of addition of renewable energy sources for power generation. Further, intelligent way of theft detection is introduced so that there could be no compromise over any energy theft. Based on the comparison of current values of supplier and consumer, power system is made secure.

In addition to this, enhanced security features for communication between suppliers and consumers in introduced for first time in power system. This will not only increase reliability of service to essential loads but also increased overall efficiency of usage of energy and capitals. Message digest algorithm based security for wireless communication between supplier and consumer make both supplier and consumer more autonomous and intelligent. Power system information cannot be altered by cyber intruder because of this type of security.

REFERENCES

[1] R. Muzzammel, M. Ahsan and W. Ahmad, "Non-linear analytic approaches of power flow analysis and voltage profile improvement," 2015 Power Generation System and Renewable Energy Technologies (PGSRET), Islamabad, pp. 1-7, 2015.

[2] H. Kanchev, D. Lu, F. Colas, V. Lazarov and B. Francois, "Energy Management and Operational Planning of a Microgrid with a PV-Based Active Generator for Smart Grid Applications," in *IEEE Transactions on Industrial Electronics*, vol. 58, no. 10, pp. 4583-4592, Oct. 2011.

[3] F. Abbas, S. Yingyun and U. Rehman, "Hybrid Energy Management System with Renewable Energy Integration," *2015 Seventh International Conference on Computational Intelligence, Modelling and Simulation (CIMSim)*, Kuantan, pp. 121-126, 2015.

[4] A.Merabet, K. Tawfique Ahmed, H. Ibrahim, R. Beguenane and A. M. Y. M. Ghias, "Energy Management and Control System for Laboratory Scale Microgrid Based Wind-PV-Battery," in *IEEE Transactions on Sustainable Energy*, vol. 8, no. 1, pp. 145-154, Jan. 2017.

[5] D. Shen, A. Izadian and P. Liao, "A hybrid wind-solar-storage energy generation system configuration and control," *2014 IEEE Energy Conversion Congress and Exposition (ECCE)*, Pittsburgh, PA, pp. 436-442, 2014.

[6] N. Javaid et al., "An Intelligent Load Management System with Renewable Energy Integration for Smart Homes," in *IEEE Access*, vol. 5, pp. 13587-13600, 2017.

[7] S. Sahoo, D. Nikovski, T. Muso and K. Tsuru, "Electricity theft detection using smart meter data," *2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Washington, DC, pp. 1-5, 2015.

[8] Gupta and A. Jain, "Intelligent control of hybrid power systems for load balancing and levelised cost," *2016 IEEE 1st International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES)*, Delhi, pp. 1-5, 2016.

[9] G. Wang, M. Ciobotaru and V. G. Agelidis, "PV power plant using hybrid energy storage system with improved efficiency," *2012 3rd IEEE International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, Aalborg, pp. 808-813, 2012.

[10] M. Bragard, N. Soltau, S. Thomas and R. W. De Doncker, "The Balance of Renewable Sources and User Demands in Grids: Power Electronics for Modular Battery Energy Storage Systems," in *IEEE Transactions on Power Electronics*, vol. 25, no. 12, pp. 3049-3056, Dec. 2010.

[11] S. Mishra, Y. Mishra and S. Vignesh, "Security constrained economic dispatch considering wind energy conversion systems," *2011 IEEE Power and Energy Society General Meeting*, Detroit, MI, USA, pp. 1-8, 2011.
[12] A. A. Putri Ratna, P. Dewi Purnamasari, A. Shaugi and M. Salman, "Analysis and comparison of MD5 and SHA-1 algorithm implementation in Simple-O authentication based security system," *2013 International Conference on QiR*, Yogyakarta, pp. 99-104, 2013.
[13] A. S. Metering, S. Visalatchi and K. K. Sandeep, "Smart energy metering and power theft control using arduino & GSM," *2017 2nd International Conference for Convergence in Technology (I2CT)*, Mumbai, pp. 858-961, 2017.
[14] S. Ojha and V. Rajput, "AES and MD5 based secure authentication in cloud computing," *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, pp. 856-860, 2017.
[15] P. Ora and P. R. Pal, "Data security and integrity in cloud computing based on RSA partial homomorphic and MD5 cryptography," *2015 International Conference on Computer, Communication and Control (IC4)*, Indore, pp. 1-6, 2015.
[16] V. Mota, S. Azam, B. Shanmugam, K. C. Yeo and K. Kannoorpatti, "Comparative analysis of different techniques of encryption for secured data transmission," *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, Chennai, pp. 231-237, 2017.
[17] M. D. A. Chawdhury and A. H. M. A. Habib, "Security enhancement of MD5 hashed passwords by using the unused bits of TCP header," *2008 11th International Conference on Computer and Information Technology*, Khulna, pp. 714-717, 2008.
[18] D. Cao and B. Yang, "Design and implementation for MD5-based data integrity checking system," *2010 2nd IEEE International Conference on Information Management and Engineering*, Chengdu, pp. 608-611, 2010.
[19] D. Ciupăgeanu, G. Lăzăroiu and M. Tîrşu, "Carbon dioxide emissions reduction by renewable energy employment in Romania," *2017 International Conference on Electromechanical and Power Systems (SIELMEN)*, Iasi, pp. 281-285, 2017.
[20] B. S. Chouhan, K. V. S. Rao and B. Kumar Saxena, "Reduction in carbon dioxide emissions due to wind power generation in India," *2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, Bangalore, pp. 257-264, 2017.
[21] R. Muzzammel, "Traveling Waves-Based Method for Fault Estimation in HVDC Transmission System," *Energies*, vol. 12, pp. 3614-3645, 2019.
[22] R. Muzzammel, "Machine Learning Based Fault Diagnosis in HVDC Transmission Lines," *INTAP 2018: Intelligent Technologies and Applications*, vol. 932, pp. 496-510, March 2019.
[23] R. Muzzammel, "Restricted Boltzmann Machines Based Fault Estimation in Multi Terminal HVDC Transmission," presented at the Intelligent Technologies and Applications, Bahawalpur, pp. 1 – 20, 2019.
[24] R. Muzzammel, H. M. Fateh and Z. Ali, "Analytical behaviour of thyrister based HVDC transmission lines under normal and faulty conditions," *2018 International Conference on Engineering and Emerging Technologies (ICEET)*, Lahore, pp. 1-5, 2018.
[25] R. Muzzammel and U. Tahir, "Analytical behaviour of line asymmetries in three phase power systems," *2017 International Symposium on Recent Advances in Electrical Engineering (RAEE)*, Islamabad, pp. 1-5, 2017.

BIOGRAPHIES OF AUTHORS

Raheel Muzzammel received his B.Sc. Electrical Engineering Degree from Department of Electrical Engineering at University of Engineering and Technology, Lahore, Pakistan and M.S Electrical Engineering Degree from Department of Electrical Engineering at University of Lahore, Lahore, Pakistan. Currently he is working as an Assistant Professor in the Department of Electrical Engineering in the University of Lahore, Lahore, Pakistan. His research interests include power systems, power system protection and power electronics.

Rabia Arshad received the Masters degree in electrical engineering from the University of Lahore, Lahore in 2016 following her BSc. in Computer Engineering from the University of Engineering and Technology, Lahore. Currently he is working as an Assistant Professor in the Department of Electrical Engineering in the University of Lahore, Lahore, Pakistan. She has an experience of more than 7 years in academia. Her research interests include wireless sensor network in communication systems.

Engr, Saba Mehmood received her MSc degree in Electrical Engineering from Government College University in 2016. She completed her graduation in EE in 2013 from FAST LAHORE. She is currently serving as a Lecturer in the Department of Electrical Engineering, The University of Lahore, Lahore. She has got four years experience of teaching various Electronics and Programming courses at undergraduate level as well as supervising many semester projects. She has also Participated in Faculty Development Workshops and Seminars on Communication Science and System.

Danista Khan is pursuing her PhD degree from The Hong Kong Polytechnic University. She received her MSc degree in Electrical Engineering from University of Engineering and Technology in 2017. She completed her BSc in Electrical Engineering from the University of Lahore in 2013. She has got five years experience of teaching various Electronics and Telecommunication courses at undergraduate level.