GU J Sci 30(4): 330-343 (2017)

Gazi University

Journal of Science

http://dergipark.gov.tr/gujs

A Novel keyless and key based Encryption Algorithm to handle Cyber Security in Microgrid Application

Jakir Hossain[1,*], Sarder Shazali Shikander[2], Eklas Hossain[3], Ramazan Bayindir[4]

[1]*University of South Florida, Department of Electrical Engineering, FL 33620, Tampa, USA.*

[2]*National Université of Science and Technologie, Islamabad, Pakistan.*

[3]*Oregon Institute of Technology, Department of Electrical Engineering and Renewable Energy, OR 97601, USA.*

[4]*Gazi University, Department of Electrical Engineering, 06500, Ankara, Turkey.*

mdjakir@mail.usf.edu[1], shazali.ali67@gmail.com[2], eklas.hossain@oit.edu[3], bayindir@gazi.edu.tr[4]

Article Info

Received: 09/10/2016
Accepted: 14/08/2017

Keywords

Cipher text
Cyber security
Microgrid
OSI-Protocol
IOT
Encryption
Decryption

Abstract

Smart grid technology, a reasonable move in modern power system, assures coveted resiliency, consistency, and the utmost efficiency of the entire grid system utilizing the cyber resources via extensive communication between the subordinate bodies. But, like other cyber communication process, the smart grid technology is now in the security concern because of the modern eavesdropping techniques. To keep the system safe and secure from the probable vulnerability, several encryption algorithms have already been developed to ascertain secure data transmission. But, the processing time of these traditional algorithms is comparatively higher and this drawback certainly endangers the system security. In this paper, the authors have introduced a short run time based secure encryption algorithm that can literally fulfil the security requirements in microgrid systems. In particular, this proposed algorithm is designed in two manners: Key-based and Key-less approaches with the elaborate delineation so that one can easily compare the security parameters, process runtime, and consistency with the current encryption algorithms. Finally, to vindicate the legitimacy of the proposed algorithm, all the results and issues have been verified in the simulation platform such as Matlab/ Simulink.

1. INTRODUCTION

Renewable energy sources have become quite popular these days, and the reasons are quite obvious: they do not require fuel like conventional energy sources, can convert infinite natural resources like sunlight (solar cells) or wind (wind turbines) into electricity, and most importantly, they do not produce any carbon or other deleterious elements that can harm the environment. In a world with fast diminishing natural resources and melting icecaps, they sound like the perfect solution to serve a power-hungry population. Then there comes the smart grid (SG) where energy generation is focused a lot on distributed energy sources (DER) [1]. These DERs are of the renewable types because of the benefits stated above. But such sources have an intermittent power generating pattern and they are not centralized in any particular spot of the grid, and thus creating numerous puzzles when it comes to state estimation (SE), planning of control and reliability schemes of the smart grid.

Now, when it comes to microgrid, a satellite system which solely depends on distributed generation, such control systems hold utmost importance. Microgrid can be dubbed as a derivative of smart grid requiring similar control and communication facilities. Therefore, to ascertain control and consistency, a resilient

[*] Corresponding author, e-mail: jakirhossain471@gmail.com

and efficient communication infrastructure is needed in the grid system to control the DER operations and thus estimate their performance.

To make all this possible, intelligent energy management systems (EMSs) are needed and their objectives and concepts can be compared to the ones of the Internet of Things (IoTs), which is capable of using the privacy and secrecy of the DER messages, the connectivity and effortless interoperability. Recently, this combined vision of IoT and SG appeared as the Internet of Energy (IoE) [1]. The distributed generation (DG) conception helps the service providers as well as consumers to reduce dependency on a centralized energy generating facility and creates opportunities for on-site/near-site generation plant placement. Generally, a microgrid uses multiple on-site distributed generation sources to maximize the generation from natural sources.

The actual microgrid studies, from the pragmatic point of view, include distributed generation (DG) planning, control of power flow, grid integration measures and power distribution concerns. Besides that, abundant approaches are established to achieve load sharing and correlated communication systems. The control procedures of microgrid system are categorized as specifically hierarchical, centralized and decentralized regarding the requirements. The decentralized control provides distributed control mechanisms and permits dealing with composite infrastructures by enabling self-directed systems. But on the other hand, it requires proper coordination between the related parts of the whole system.

The hierarchical control uses a master-controller as base to weigh the generating and consuming parts which are in terms of real power as well as reactive power flows. Then, voltage's reactive power and frequency's real power yield the essential power of the microgrid, in both real and reactive terms. So, the master controller has to manage the droop features of frequency or voltage with a view to controlling the power flow [2]. Fig. 1 represents a schematic view of multiple DERs which are connected to the distribution system in the format of IEEE 3. Here, in this figure, a converter interfaced the DER with a local load. A DC voltage source is connected in series to a voltage source converter and an RL filter is used to represent each DER.

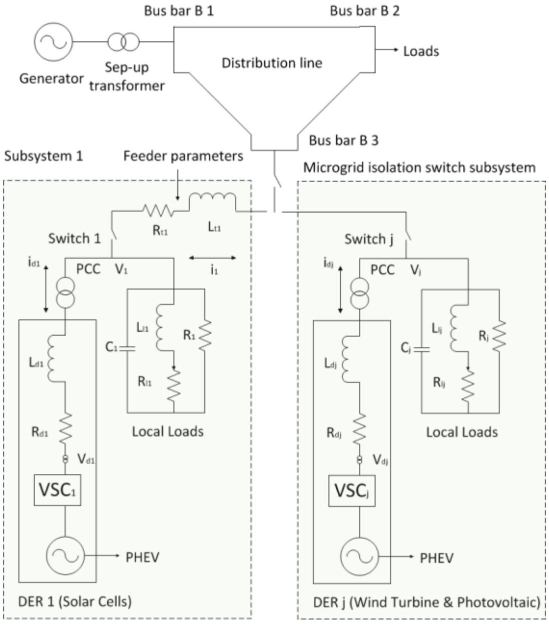


Figure 1. *Block diagram representing Microgrid using multiple DERs [1].*

According to the theory of both Kirchhoff's voltage and current law, the equations of the DERs can be stated such as

$$i_{lj} = (v_j - R_{lj}i_{lj}) / l_{lj} \qquad (1)$$

$$i_{dj} = (v_{dj} – R_{dj} – v_j) / L_{dj} \qquad (2)$$

$i_{tj} = (v_j - R_{tj}i_{tj} – v_{j+1}) / L_{tj}$ (3)
$vj = (- v_j / R_j – i_{lj} + i_{dj} – i_{tj}) / C_j$ (4)

To delineate the case, firstly, microgrid system operation, microgrid communication system, layered communication system model, microgrid security issues will be described in this paper. After that, current system vulnerabilities, existing cyber security approaches will be illustrated to figure out the necessity of further research to enhance the security issue. And finally, the proposed algorithm and the supporting simulation result will be manifested to establish the strength and robustness of the projected algorithm.

2. MICROGRID SYSTEM OPERATION

A model of modern smart grid communication system, depicted in Fig. 2, shows the integration of several regional control centres [7]. Here, in this structure, each of control centers supervises the major operation of multiple power plants and substations which are connected to the major system. Basically, the smart grid communication system is layer structured and this performs both data collection and control of electricity delivery [6]. Alternatively, the regional control center supports numerous systems like metering system, data management operation, data acquisition control, and power market & system operations.

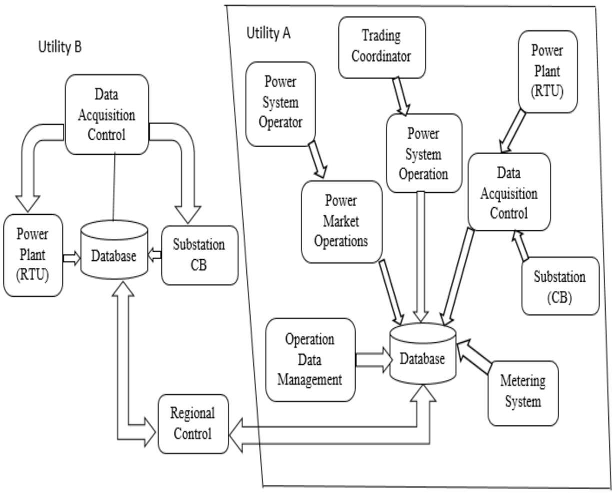


Figure 2. *Microgrid Communication Network [1].*

In particular, the substations contain various accessories which are Remote Terminal Units (RTU), Circuit Breaker (CB), Human-Machine Interfaces (HMI), communication devices such as switches, hubs, and routers, log servers, data concentrators, and a gateway for maintaining protocol. Also there are Intelligent Electronic Device (IED) are field devices [8, 18-23], instrument transducers, tap changers, circuit re-closers, phase measuring units (PMU), and protection relays are used in the substations [5].

3. MICROGRID COMMUNICATION SYSTEMS

A modern smart grid is the combination of several subsystems. In straight word, it is actually a network of certain networks. The communication networks used in modern smart grid can contain devoted or overlaid land mobile radios (LMR), microwaves, optical fibers, power line communications (PLC), serial links like RS-232/RS-485, wireless local area networks (WLAN) or such kind network which is the combination of various media like these [10]. Both working and marketable needs of electric utilities necessitate such kind of data communication network which can provide top-notch performance. Not only that, it can support standing features and future necessities. It is really crucial to design such kind of network architecture which is cost-effective and reliable. For electric system automation both the scopes and puzzles of hybrid network construction are discussed in [11]. Internet dependent Virtual Private Network (VPN), satellite communication, wireless communications like wireless-sensor-networks, WiMax and wireless mesh-networks and finally power line communication are also discussed. At present smart grid communication network is such kind of organised structure for electrical practicalities which is intended to implement a new communication technology for automation and effective direct decision making process. Fig. 3 illustrates a standard smart grid communication system architecture with all necessary possible units facilitates the security purpose.

It is to be mentioned that Advanced-Metering-Infrastructure (AMI) answers which can be meshed or point to point with short and long range local communications [4, 15]. Choices for back-haul keys might be fiber, wireless-broadband, or broadband over power line. The probable answers contain WiMax, WLAN, WSN, cellular and LMR, subject to the consistency, output, and coverage preferred by the utility. Each of the overhead choices has their benefits and drawbacks, but what is reliably correct of any and all of the answers is the requirement to have a accessible security solution.

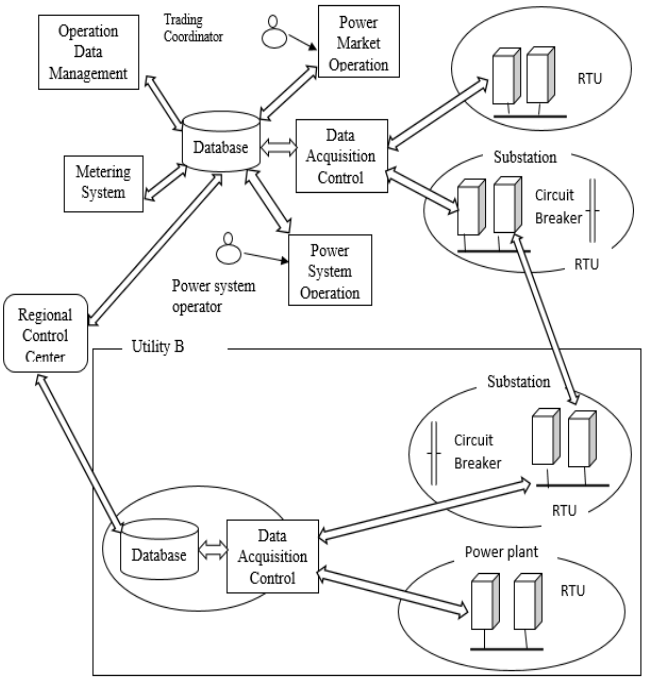


Figure 3. *A Smart Grid Communication System [9].*

4. LAYERED COMMUNICATION SYSTEM MODEL

In data communication, there are some protocols through which data is transferred through the medium. Simply, protocols define the format of the message and also define in which order the messages will be sent and received through network bodies, and which actions should be taken on message transmission, receipt. Since modern communication system is designed in several layered approaches, then the standard OSI is a layered based network structure which contains seven layers. They are Application layer, Presentation layer, Session layer, Transport layer, Network layer, Data link and Physical layer. The Application layer is situated on the top of the OSI model. Commonly, Application layer protocols are used to interchange data between programs running on the source and destination hosts in the communication network. There are many Application layer protocols used in modern times such as FTP, SMTP, HTTP, and DNS etc. In the next layer, the job of the presentation layer is to define the format of the data which to be exchanged between applications and it also offers application programs a set of data transformation services [16]. Then, the session layer normally switches the exchange of information to initiate dialogs, keep them active, and to restart sessions which are being disrupted or idle for a long period of time in the communication process. After that, the transport layer is mainly responsible for the overall end-to-end transfer of application data (logical communication between processes). Transport layer protocols are TCP, UDP. In next layer, the main task of network layer is to specify the address and processes that enable the data to be packaged and transported (logical communication between hosts) through the transport layer. Network layer protocols are IP, RIP and OSPF etc. Next, data-link layer is responsible for transferring datagram from one node to adjacent node over a communication link. The role played by OSI Data Link layer is to prepare Network layer packets for transmission and to control access to the physical media. Flow Control, Error Detection and Error Correction protocols used in this layer are TDMA, FDMA, Slotted ALOHA, CSMA, CSMA/CD etc [17]. The part of the OSI Physical layer is to encode the binary digits that characterise Data Link layer frames into signals and to transmit and receive these signals across the physical media copper wires, optical-fibre, and wireless that connect network devices [8]. Table 1 represents the layered security protocols.

Table 1. *OSI System Layered Security Protocols*

Layer	Security Protocol	Application	Confidentiality	Integrity	Authentication
Application	WS-Security	Document	Yes	Yes	Data
	PGP/GnuPG	Email	Yes	Yes	Message
	S/MIME		Yes	Yes	
	HTTP Digest Authentication	Client Server	No	No	User
Transport	SSH		Yes	Yes	Server
	SSI/TLS		Yes	Yes	
Network	IPSec	Host-to-Host	Yes	Yes	Host
Link	CHAP/PAP	Point-to-point	No	No	Client
	WEP/WAP	Wireless Access	Yes	Yes	Device

5. MICROGRID SECURITY ISSUE

According to the theme of the Electric Power Research Institute (EPRI), cyber security is the biggest challenges that are faced in smart grid deployment which is presented in [12]. The EPRI report shows that cyber security is a serious issue due to the growing number of potential cyber attacks and events occurred in this critical sector since it becomes interconnected more and more in recent times. Cyber-security has to report not only deliberate occurrences but also from irritated personnel, industrialised spying, or extremists [8, 18-20]. But, unintentional data structure which is due to consumer mistakes, apparatus failures and natural tragedies is mainly focused.

Weaknesses easily permit an attacker to intrude in a network, gain entree to the control software, and modify the load settings to sabotage the grid in unexpected means [3]. In recent years, there are many administrations are operational on the improvement of microgrid security necessities including North American Electrical Reliability Corporation Critical Infrastructure Protection (NERC-CIP), International Society of Automation (ISA), IEEE 1402, National-Infrastructure-Protection-Plan (NIPP), and National-Institute-of-Standards-and-Technology (NIST) which have a number of smart-grid cyber-security programs on proceeding to implement a reliable and secure smart grid communication system [8, 18-20]. There is one thing which is dependable among various standard organisations that the security of the smart-grid powerfully relies on several issues: authentication, authorization and finally privacy technologies. Wired links should be secured with various actions like firewalls and virtual private network technologies. Possible security threats of microgrid/smart-grid network which increase attack surface and risk of operation have been pointed out in Fig. 4 in a quick preview.

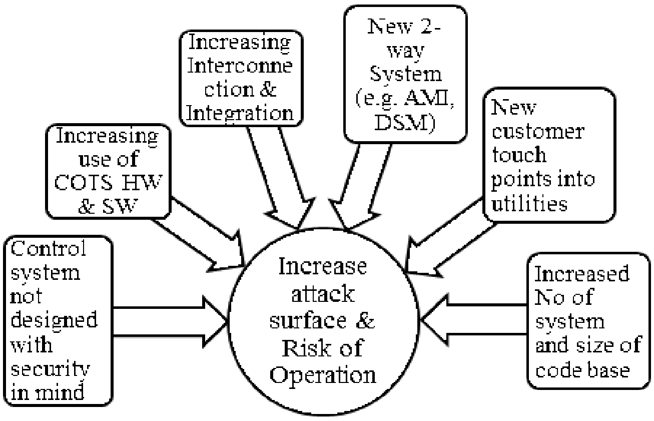

Increasing Interconne ction & Integration
New 2-way System (e.g. AMI, DSM)
Increasing use of COTS HW & SW
New customer touch points into utilities
Control system not designed with security in mind
Increase attack surface & Risk of Operation
Increased No of system and size of code base

Figure 4. *Microgrid Security Threats [1].*

6. CURRENT SYSTEM'S VULNERABILITY

Most control communications in the microgrid will occur over an Internet-Protocol (IP) network, and therefore, the control system network will have the same weaknesses that happen in traditional IP networks. These weaknesses are briefly discussed in [13]. The microgrid control system may also have weaknesses that are more precise to (Industrial control systems) ICSs. COTS hardware and software are used in the microgrid system without any customization, as a result, if any program that is set to attack the whole system is present. Then, there is a chance to be attacked by the attacker; in consequence, microgrid system faces a great difficulty in using COTS hardware and software. When more interconnection and integration approaches appear in the microgrid system, then it becomes risky for secure data communication among them. While there is an interconnection among several clients, then the attacker gets the opportunity to interrupt in the communication medium, since the communication medium is vulnerable. In Table 2, some common vulnerabilities of IP network have been enlisted. Specific cyber security concerns within AMI system from the dependence on embedded systems, device deployments in large scale, and constrained network bandwidth limit the security monitoring approaches. Since the meter allows interactions from multiple parties, specifically consumers and utilities, it will likely need to support remote access which could be abused by an attacker.So, a meter must be able to authenticate itself to the headed devices, it must maintain some shared key or password within the meter. After depicting the table, Fig. 5 shows the unsecure situation in network.

Table 2. *Some Common Weaknesses of IP Network [10]*

Vulnerability Category	Description
Eavesdropping	Network communications are inactively supervised for data with authentication IDs. For illustration, a foe uses monitoring software and native IP network access to record the user data between a consumer and server, as well as the consumer's personal information's that are exchanged in plain-text.
Man-in-the-middle (MITM)	Network communications between two authentic groups are dynamically intercepted. A foe thus achieve verification IDs and data and then cover-up as a authentic identity. For illustration, foe uses applications to make a consumer verification ID, system identifies the foe's information system is the authentic server and vice-versa. The foe is then able to access, record, and change all user data communication between the consumer and server.
Masquerading	A legal consumer is mimicked, letting a foe to acquire confident illegal privileges. For illustration, a foe is able to steal the personal authentic information's for a valid consumer. The foe applies these information's to gain access to the data base.

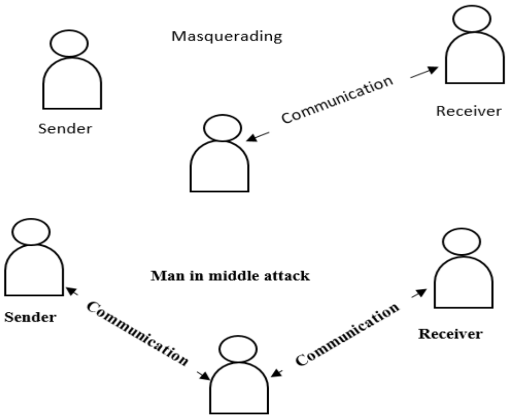


Figure 5. *Microgrid Security Threats [5].*

Privacy issues currently hinder consumer acceptance due to concerns that data will be provided to marketers, law enforcement, or other third parties. Another task is performed by AMI is that it enables Demand Side Management (DSM) whose objective is to exercise direct/indirect control over consumer power consumption in smart metering system. Since customers are connected with this system through Metering system and the amount of consumption is obtained through the meter reading, so it is important to keep data private from public access. Integrity refers to the prevention of hidden alteration of information by unlicensed adversary or systems.

When the system grows larger that means when we need to implement many systems all together and the system integrated among them through several coding technique, then it merely happens that attacker tries to inject one of this heavy system. As a result, one of the less secure portions may be hacked. So, the main concern is to minimize the size of the system and in less coding technique. Since the connected systems exchange data through the networks, then it is the first choice of the attacker to attack through any weak point of the system and they try to find out the weak point of the system. In several cyber-attacks, worm invasions have upheld to negative influence on critical network set-ups. Such kind of intimidations have mostly been being the consequence of leaving a communication network exposed to threats from the Internet [18-20].

7. EXISTING CYBER SECURITY APPROACHES

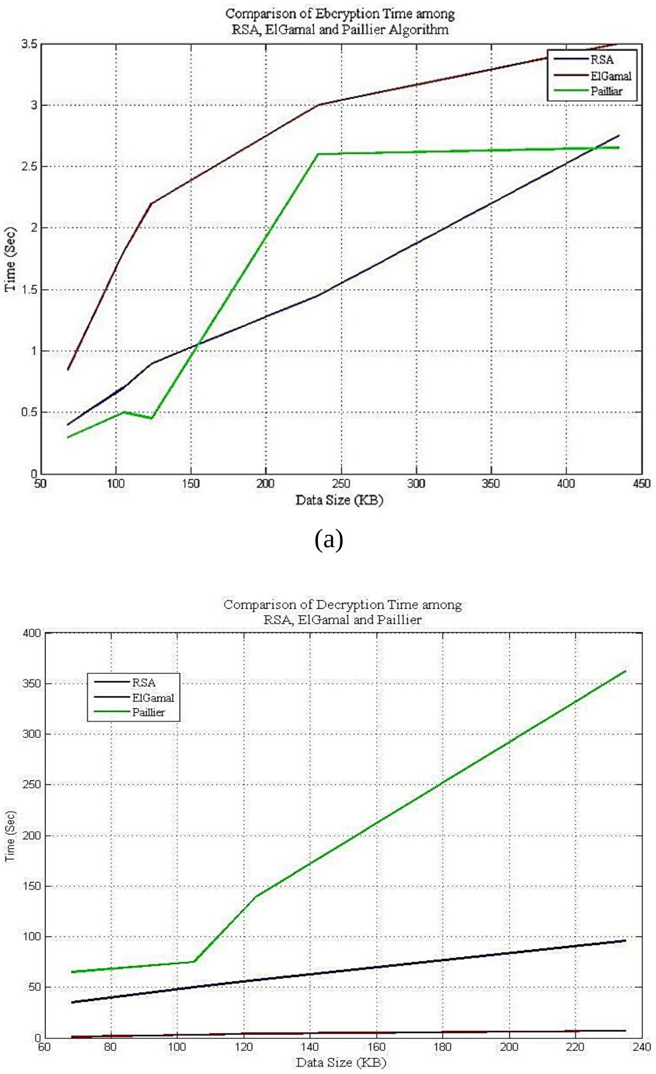
To prevent Cyber-attack, the following approaches are used for security purposes worldwide. They are RSA, ElGamal and AES etc. Their working criteria and performance are measured through several researches and hence, they are used globally. The cryptographic methods are widely classified as symmetric and asymmetric. In symmetric methods, encryption and decryption keys are same. But, often decryption key is easily calculated from the encryption key for various purposes and approaches. The problem with symmetric method is that the participants have to share a secret key in a secure way which is difficult to execute [14]. Asymmetric methods are being implemented to solve the problem and this is the main concern in key distribution by using a pair of keys. It is practically infeasible in general purpose to estimate the decryption key given only the knowledge of cryptographic algorithm and the encryption key. RSA is one of the oldest and most practically used encryption algorithms in security issue. In RSA, the key pair is derived from the production of two prime numbers which are chosen according to the special rules. RSA is an asymmetric key algorithm where a message is encrypted to a cipher text by applying a public key and decrypted to plain original text by using a private key that is calculated in this approach.

RSA algorithm is likewise M = actual message, C = cipher text, e = public key, N = modulus public key, d = private key. Now, if we want to apply the encryption and decryption process, the procedure will be the following.

$$C = (M^e) \bmod N \tag{5}$$

$$M = (C^{d}) \bmod N \qquad (6)$$

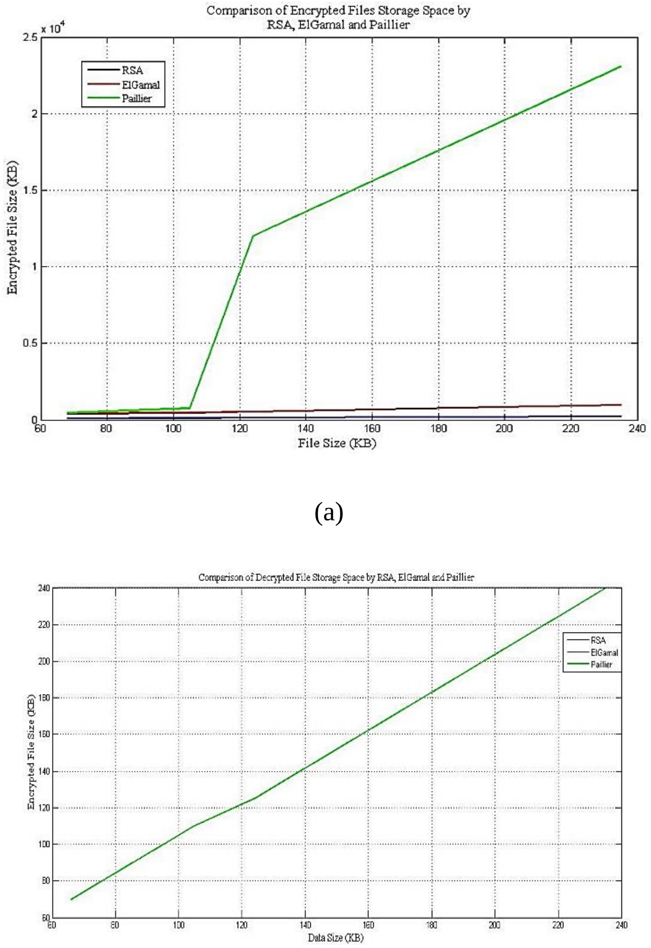
Here, Equation (5) represents the cipher text equation and Equation (6) represents the decryption equation. Since decryption is kept private, then it is protected from the attacker. On the other hand, since RSA is an asymmetric algorithm, then it is quite tough to break the cipher for the hackers. SO, it requires much effort for breaking the RSA encrypted cipher for the attacker. Similarly, in ElGamal method, both the plain text and the key are encrypted in a symmetric manner, so the sender and the receiver can estimate the security key randomly and only both of them know the security system. As a result, the attacker can’t know about the security key and can’t break it. The comparison between RSA and several encryption algorithms with respect to encryption, decryption time and file is shown in Fig. 6. From the graph that shows the comparison among the traditional standards encryption algorithms but their run time is pretty much high. So, it is not easy for the hacker to break the system. And for this major reason, these encryption algorithms are being used for many years. RSA has time complexity of O (log (n) 3), so it takes much time. In such cases, where we don’t need complexity issue like in microgrid, we can propose a less runtime based encryption algorithm, since here data changes rapidly and then we need very short decryption time. Here, we propose two types of algorithm where the first one is key based and another one is keyless.



(a)

(b)

Figure 6. *Comparison among RSA, ElGamal, and Paillier in a) Encryption and b) Decryption Time.*



(a)

(b)

Figure 7. *Comparison among RSA, ElGamal and Paillier in a) Encrypted and b) Decrypted File Size.*

8. PROPOSED CYBER SECURITY APPROACHES

8.1. Proposed Key based Algorithm

According to the facts discussed earlier, we have proposed a new encryption algorithm that requires keys but not similar to RSA approach. The proposed algorithm features are showed below.

Primary key 1 = B (7)
Primary key 2 = S (1< S <= B/2) (8)

Suppose, our data is about 32 bits which is like this binary form 10111010101101110101000101100110. So, if we want to use this approach to apply encryption and decryption, we'll have to apply these actions like Block generation, shifting, consolidation. Here, the first approach is block generation: segmentation of the data series into B size blocks. If B = 8, then the data will be generated like the following block.

10111010 10110111 01010001 01100110 (9)

Now, we need to shift each block S times to right or left. Then, the data pattern will be like following, if S = 3, each block would be in (right shifted) this form

01010111 11110110 00101010 11001100 (10)

Now, in consolidation phase, we will have to combine all blocks and then add flag bits. After combining the blocks all together, our data will be like the following pattern.

01010111111011000101010110011 00 (11)

We will add 2 flag bits which are defined like First bit = Odd length or Even Length it'd be 0 = Even; 1 = Odd and the Second bit = Directional bit which will 0 = Left shift; 1 = Right Shift. So the data will be looking like.

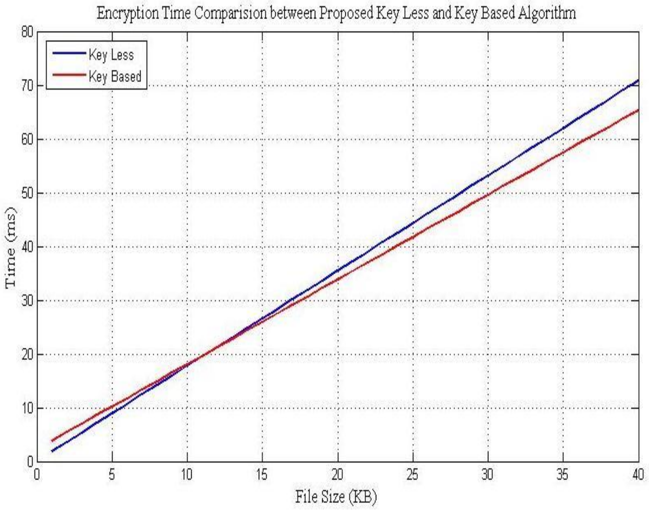
01 + 0101011111101100010101011001100 (12)

In equation (8), the first flag bit is for even length flag bit and the next one is for right shift flag bit. Now we have done and our final data will be like this.

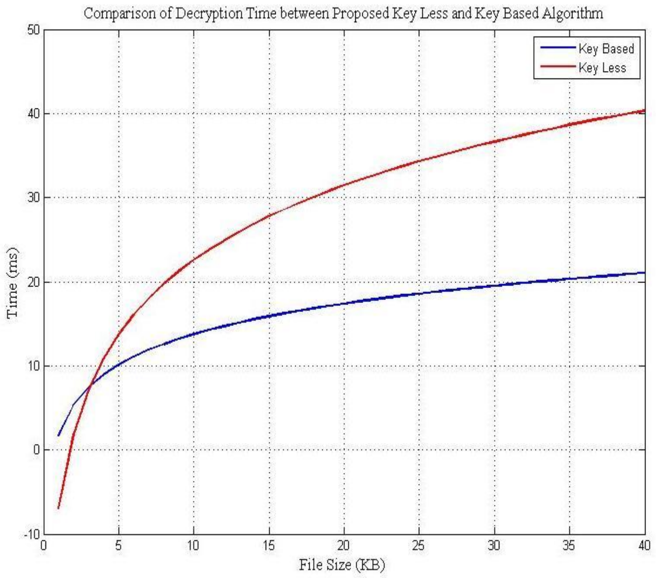
010101011111101100010101011001100 (13)

8.2. Proposed Key less Algorithm

In this proposal, we have proposed an algorithm where we avoid key factor for encryption and decryption. Since it is independent of key, so the main encryption process is secured. Though its runtime is very short, it is helpful for microgrid purpose because the data changes so fast here. In this approach, the algorithm gives such kind of performance due to short range of data. These are represented in Fig. 8. In like manner, Fig. 9 represents the time comparison between RSA and our proposed algorithm.



(a)



(b)

Figure 9. *Comparison among RSA, Elgamal, and Paillier in a) Encrypted and b) Decryption File Size.*

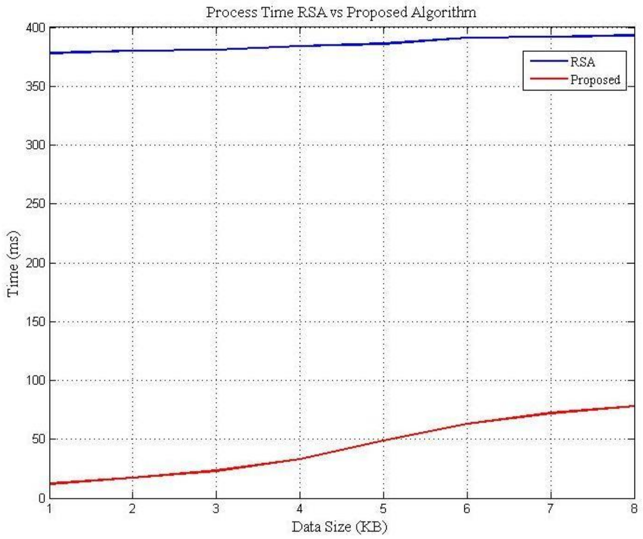


Figure 10. *Time Comparison between RSA and Proposed.*

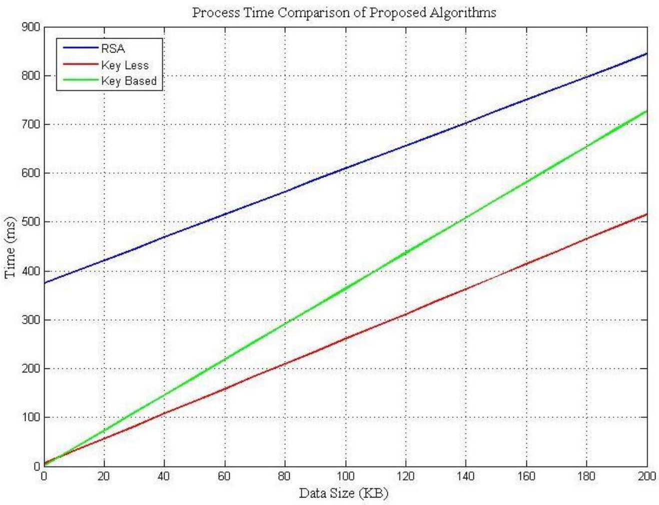


Figure 11. *Process time comparison among RSA, key based and key less algorithm.*

9. SIMULATION RESULTS

Here, to analyze performance of the proposed algorithm, we simulated several test cases through which we can get some comparison between our proposed algorithm and the RSA algorithm. The simulation result is shown in the Fig. 10. In this graphical illustration, we have seen that the total process time in RSA is comparatively high since it uses asymmetric encryption system through different keys whose size is comparatively bigger due to security issue. On the other hand, in our proposed algorithm, the processing time is very short. Though its process time is short, it is applicable in microgrid communication system purpose since in such kind system data changes rapidly in a short time interval. So, in such case, we need this type of encryption algorithm which can process the sent data very fast, before the attacker can recognizes the pattern of the data. With a view to ensure high security issue, RSA algorithm uses large key size. Though it increases security level, it increases both time and space complexity. According to the General Number Field Sieve (GNFS), one of the fastest classical factoring algorithms we have found the strengths of RSA for especially large key are relatively high. As a cryptographic algorithm has n bit keys then it can ensure k bits strength. The most effective standard algorithm in number theory for factoring integers greater than 100 digits can be expressed as below in equation (14).

$$\mathbf{exp}\left(\left(\sqrt[3]{\frac{\mathbf{64}}{\mathbf{9}}}+\boldsymbol{o}(\mathbf{1})\right)(\boldsymbol{Inn})^{\frac{1}{3}}(\boldsymbol{InInn})^{\frac{2}{3}}\right)=\boldsymbol{L_n}\left[\frac{\mathbf{1}}{\mathbf{3}},\sqrt[3]{\frac{\mathbf{64}}{\mathbf{9}}}\right] \tag{14}$$

Using this criteria any breaking algorithm will have to use 2k operations required to break the security issue through Brute Force manner.

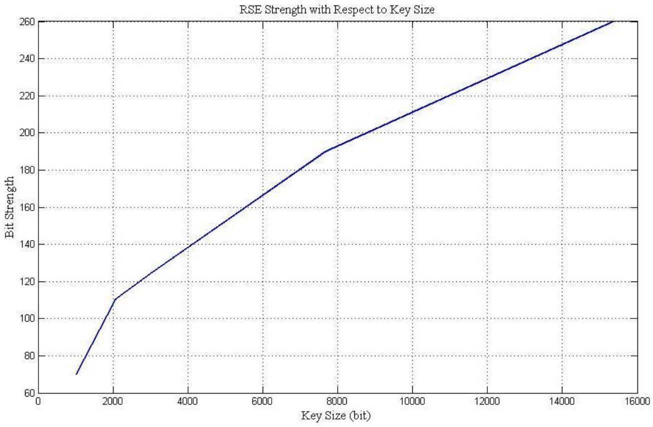


Figure 12. *RSA bit strength with respect to key size.*

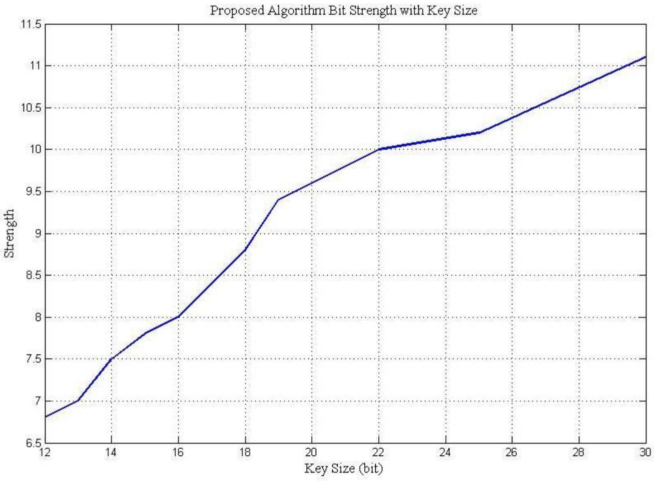


Figure 13. *Proposed algorithm strength with respect to key size.*

Here, operation is a fuzzy term. Hence according to the GNFS equation in eqn. 14 we have found such strength of both RSA algorithm and proposed key based algorithm which are shown in Fig. 11 and 12 respectively. That means if we use RSA-1024 which provides 80 bits strength so it is required 280 operations through Brute Force approach using all its probable 21024 keys. Where our proposed algorithm uses fewer key so it is seen that the strength is not as much as RSA provides but it can be acceptable in microgrid operation as here data changes rapidly in accordance with power production.

10.CONCLUSION

A safe and secure microgrid communication is fully dependent on optimal security algorithm which can ensure the proper cyber security of the microgrid communication. Traditionally, several approaches are used in such perspective issue, but for better performance, we have introduced a much robust algorithm which is very much efficient for achieving our goal in secure microgrid communication. Here, the proposed algorithm ascertains smaller process time than that of the traditional encryption algorithm like RSA. Though our algorithm strength is not as high as RSA, it is much appreciable for the aspect of microgrid security issue. Apart from the theoretical details, to vindicate the authenticity of the proposed algorithm, all the results and issues have been verified in the simulation platform such as Matlab/ Simulink.

REFERENCES

[1] M. M. Rana and L. Li, "Microgrid state estimation and control for smart grid and Internet of Things communication network," in *Electronics Letters*, vol. 51, no. 2, pp. 149-151, 1 22 2015. doi: 10.1049/el.2014.3635

[2] E. Kabalci, E. Hossain and R. Bayindir, "Microgrid test-bed design with renewable energy sources," *Power Electronics and Motion Control Conference and Exposition (PEMC), 2014 16th International*, Antalya, 2014, pp. 907-911. doi: 10.1109/EPEPEMC.2014.6980622

[3] J. O. Petinrin and M. Shaaban, "Smart power grid: technologies and applications," *Power and Energy (PECon), 2012 IEEE International Conference on*, Kota Kinabalu, 2012, pp. 892-897. doi: 10.1109/PECon.2012.6450343

[4] Anthony R. Metke. "Smart grid security technology", 2010 Innovative Smart Grid Technologies (ISGT), 01/2010

[5] M. Azab and M. Eltoweissy, "CyPhyMASC: evolutionary monitoring, analysis, sharing and control platform for smart grid defense," *Information Reuse and Integration (IRI), 2014 IEEE 15th International Conference on*, Redwood City, CA, 2014, pp. 639-645. doi: 10.1109/IRI.2014.7051950

[6] Wenye Wang, Yi Xu, Mohit Khanna, A survey on the communication architectures in smart grid, Computer Networks, Volume 55, Issue 15, 27 October 2011, Pages 3604-3629, ISSN 1389-1286, http://dx.doi.org/10.1016/j.comnet.2011.07.010.

[7] T. Mehra, V. Dehalwar and M. Kolhe, "Data communication security of advanced metering infrastructure in smart grid," *Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on*, Mathura, 2013, pp. 394-399. doi: 10.1109/CICN.2013.87

[8] Y. Yan, Y. Qian, H. Sharif and D. Tipper, "A survey on cyber security for smart grid communications," in *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 998-1010, Fourth Quarter 2012. doi: 10.1109/SURV.2012.010912.00035

[9] C. H. Hauser, D. E. Bakken, A. Bose, “A failure to communicate”, *IEEE Power and Energy Mag.*, pp. 47-55, Mar- Apr, 2005.

[10] P. McDaniel and S. McLaughlin, “Security and privacy challenges in the smart grid,” *IEEE Security & Privacy*, vol. 7, pp. 75-77, 2009.

[11] V. C. Gungor and F. C. Lambert, “A survey on communication networks for electric system automation,” *Computer Networks*, vol. 50, pp. 877-897, 2006.

[12] G. Carl, G. Kesidis , R. R. Brooks , and R. Suresh , “Denial-of-service attack- detection techniques ,” *IEEE Internet Computing*, vol. 10, pp. 82-89, 2006

[13] K. Stouer, J. Falco, and K. Scarfone, “Guide to industrial control systems (ICS) security," *NIST Special Publication (SP) 800-82*, NIST, Gaithersburg, MD, June 2011.

[14] J. Y. Kim and H. K. Choi, "An efficient and versatile key management protocol for secure smart grid communications," *2012 IEEE Wireless Communications and Networking Conference (WCNC)*, Shanghai, 2012, pp. 1823-1828. doi: 10.1109/WCNC.2012.6214081

[15] N. Goel and M. Agarwal, "Smart grid networks: A state of the art review," *Signal Processing and Communication (ICSC), 2015 International Conference on*, Noida, 2015, pp. 122-126. doi: 10.1109/ICSPCom.2015.7150632

[16] C. Ware, "The OSI network layer: standards to cope with the real world," in *Proceedings of the IEEE*, vol. 71, no. 12, pp. 1384-1387, Dec. 1983. doi: 10.1109/PROC.1983.12782

[17] TCP OSI model, data link layer protocols http://teachweb.milin.cc/datacommunicatie/tcp_osi_model/data-link_layer.htm.

[18] Kounev, Velin, “Secure real-time smart grid communications: a microgrid perspective.*” 2015, Doctoral Dissertation, University of Pittsburgh*. http://d-scholarship.pitt.edu/25888/

[19] Boss, Scott Russel, “Control, perceived risk, and information security precautions: external and internal motivations for security behavior.*” 2007, Doctoral Dissertation, University of Pittsburgh*. http://d-scholarship.pitt.edu/8566/

[20] S. T. Zargar, J. Joshi and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks," in *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2046-2069, Fourth Quarter 2013. doi: 10.1109/SURV.2013.031413.00127

[21] N. Sakib, J. Hossain, H. I. Bulbul, E. Hossain and R. Bayindir, "Implementation of unit commitment algorithm: A comprehensive droop control technique to retain microgrid stability," 2016 IEEE International Conference on Renewable Energy Research and Applications (ICRERA), Birmingham, 2016, pp. 1074-1079. doi: 10.1109/ICRERA.2016.7884499

[22] I. Colak, E. Hossain, R. Bayindir and J. Hossain, "Design a grid tie inverter for PMSG wind turbine using FPGA & DSP builder," 2016 IEEE International Power Electronics and Motion Control Conference (PEMC), Varna, 2016, pp. 372-377. doi: 10.1109/EPEPEMC.2016.7752026

[23] Hossain, Jakir, Nazmus Sakib, Eklas Hossain, and Ramazan Bayindir. "Modelling and Simulation of Solar Plant and Storage System: A Step to Microgrid Technology." International Journal of Renewable Energy Research (IJRER) 7, no. 2 (2017): 723-737.