A SCADA Intermediate Simulation Platform to Enhance the System Security

AAmir Shahzad[#1], Naixue Xiong*[2] (IEEE Member), Muhammad Irfan[#3], Malrey Lee[#4],
Shahid Hussain[#5](IEEE Member)

[#]561-756,Center for Advanced Image and Information Technology, School of Electronics
& Information Engineering, & Department of Computer Engineering,
Chon Buk National University, 664-14, 1Ga, Deokjin-Dong, Jeonju, Chon Buk, Korea
[1]mail2aamirshahzad@gmail.com, [3]irfanview2@gmail.com, [4]mrlee@jbnu.ac.kr, [5]shahiduop@jbnu.ac.kr

*The School of Optical-Electrical and Computer Engineering, University of Shanghai for Science
and Technology, Shanghai, 200093 China
[2]xiongnaixue@gmail.com (Corresponding Author)

Abstract— **SCADA (supervisory control and data acquisition) systems are increasing rapidly in the terms of uses and deployments in real time industrial processing, approximately all over the world. To fulfill, the underlying advanced acquirements of industrial process; the SCADA systems are gaining and deploying more advance features for infrastructural developments, from arena of information technology (IT). Now days, the SCADA systems are also connected with several open networks and allow the transmission of data (bytes) geographically, within local area networks (LANs)/wide area networks (WANs) over internet using "transport control protocol (TCP)/internet protocol (IP) and others". With the increasing of SCADA system connectivity with number of open networks or/and protocols, several organizations included "dnp.org, trianglemicroworks,Inc, NS network solutions, ASE-systems, modbus.org, fieldbus.org and others", have been deploying the security mechanisms to secure the communication of SCADA systems as part of industrial control systems (ICSs). In proposed study, based on existing security analysis of SCADA systems, the security implementation via cryptography mechanism has been placed between SCADA nodes during transmission of bytes. The "secure cryptography intermediate node (SCIN)" has been situated between SCADA communication nodes during transmission. Each time communication has been occurred between participated nodes, bytes are passed through SCIN which provides two-way secure communication link or channel against attacks.**

Keywords- **Supervisory Control and Data Acquisition System, SCADA Security, Secure Cryptography Intermediate Node, Cryptography Approaches, Simulation Test**

I. INTRODUCTION

Supervisory control and data acquisition (SCADA) Systems have been used number of tools or simulation tools to simulate the field devices or nodes in network communication. Each tool has specified acquirements during device configuration and support limited number of proprietary/non- proprietary protocols. Few SCADA simulation tools are free of cost, mean they provide free license versions and some provide limited session license or license key including ASE 2000 testset and Test Harness, with several types of testing or testing features.

Applied system engineering (ASE) 2000 is a protocol analyzer and testing tool for SCADA system and developed by applied system engineering, Inc. Applied system engineering (ASE) 2000 version 2 is new version released by applied system engineering. Inc, with exiting features from version 1 and also having new features, according to the demands of Industrial users in all over the world. ASE2000 has been developed for SCADA system with core emphasizing on protocols or SCADA protocols such as DNP3, IEC 870-5-104 and Modbus, etc. ASE2000 provides full supported features, for approximately 80 protocols, both for SCADA serial and network based communication sets or testsets. ASE2000 has three main modes for operation test set such as line monitor, master terminal simulation, and remote terminal simulation with exchange and task operation modes [5].

Test Harness is a graphical simulation software for SCADA supported protocols such as DNP3 LAN/WAN, Modbus, IEC 60870-5-101 with series, etc, and used to simulates the master station and remote station or vice versa. Distribute network protocol (DNP3) and other SCADA protocols, and their communication are fully supported by Test Harness simulation tool. Test Harness also provides limited session license key for device configuration and supports various types of testing [6].

II. MATERIALS AND METHODS

In research [10], the SCADA architecture and security issues have been reviewed and most common threads and vulnerabilities scenarios are highlighted, which are commonly present in SCADA system [7, 20] such as proprietary protocols interconnectivity with open networks, stations connectivity with internet, utilities instability, internet terrorism, open information for hacking/ terrorism and open tools, etc [11, 14, 15]. Some recommendations such as proper security plan, security polices, usage of authentication protocols, password management, remote access through security protocol (VPN, PKI and encryption), wireless communication management, OS management (between vendors proprietary and open protocols), security updates and patches, communication network security (using firewalls DMZs, an disaster recovery and backup, intrusion detection and prevention system) and antivirus, are provided for SCADA security enhancements during communication. Encryption mechanisms such as data confidentially and integrity, are also used for exchange information securely between SCADA nodes [1, 4, 17]. The above recommendations significantly reduce the SCADA vulnerabilities and provide protection against attack/thread [7, 12, 16].

Cyber security issues have been increasing in SCADA communication due to large connectivity with non-proprietary networks over internet. Several safety recommendations are reviewed that would be consider as a strong approach against attacks/threads and the tools/software are used to manage the risk available in SCADA architecture. The potential security solutions included TLS/SSL, IPSec, object security, encryption and authentication, and other methods, are employed to improve the security, reliability and reduce the SCADA platform weakness against vulnerabilities [8, 9, 18].

III. PERFORMANCE MEASUREMENT AND DISCUSSION

In SCADA testbed, network nodes have been configured and bytes are transmitted number of times during abnormal scenario or case of external attacks. The performance results, which have been measured during normal communication, evaluate the security solutions or proposed security implementations [2, 3, 19]. In figure 1, four nodes have been connected with main controller or master station in testbed during bytes transmission. In network topology, only main control is configured and permitted to share information with connected nodes. Mean that sub-nodes have no permission to exchange information between them, but in case of critical situation, these connected nodes are able to transmit information 19, 20].

The testbed experiments have been run approximately 38 times and security performance is measured in both cases; with and without security implementation, at each end of SCADA simulation tools. In table 1, the first or initial experiment or experiment no.0 is not listed because this experiment is counted for configuration and setup purposes, and also used to check either network nodes are properly connected with main node or main controller. The screen shots 1 and 2 in Appendix: A, show the SCADA simulation tools interfaces during configuration and setup. Each time bytes have been transmitted between main controller and network nodes or vice versa in case of response bytes only, first pass to secure cryptography intermediate node (SCIN), which is located intermediately between connected nodes, for security check. The SCIN maintain two directories within each node, one for sending and other for receiving during bytes transmission or bytes transmission from and to via SCADA simulation environments (tools). The sending bytes have been passed to SCIN sending directory, where information is storage and security mechanism is employed before transmitting to target node. Upon receiving, the bytes are stored and treated with security mechanism for security check or as a check point to verify the authentication, integrity, confidentiality and non repudiation services before received and used by simulation tools. The table 1 shows the overall information that has been taken during security implementation using cryptography or/and during deployment of secure cryptography intermediate node (SCIN).

In table 2, the first column shows the number of successful experiments during attack detection within testbed. The next four columns that are distributed in two clauses or in the format: (ASE Testset; Test Harness), show the ratio (%) of attack detection included authentication (A), confidentiality (C), integrity (I) and non repudiation(R) attacks, successful (S) or non-successful (N), with security implementation at each end of SCADA Simulation tools included ASETestset and Test Harness. While remaining four columns show the attack detection ratio (%) without security implementation (proposed implementation).The highlighted fields in table 2, show the attack detection (%) that have been detected partially during testbed abnormal communication. More detail related with number of times, attack detected with and without proposed security implementation is depicted in table 3.

The table 4 shows the detail of security ratio (%) that has been calculated or observed basis on attack impact ratio (%) and the total attack impact is calculated basis on attack detection ratio (%), while table 5 show the average performance ratio (%), during abnormal communication with implementation of proposed security solution. The table 6 shows the results basis on attack detection ratio (%), while table 7 shows the average performance ratio (%), during abnormal communication without security implementation.

The performance graphs 1, 2 and 3; show the level of attack detection or number of times attacks detected, at each end of ASETestset, while performance graphs 5, 6 and 7; show the attacks detection during abnormal transmission of Test Harness, as a part of SCADA simulation tools. The graphs 4 and 8 show the propagation delay that has been computed by the implementation of Solution^1 and Solution^2 during normal communication.

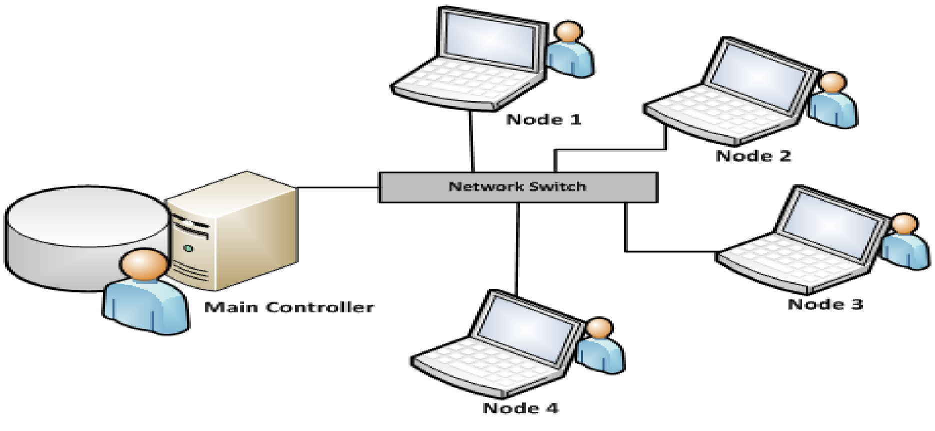


Fig 1. Testbed Setup

TABLE 1. Secuity Implementations via Cryptography

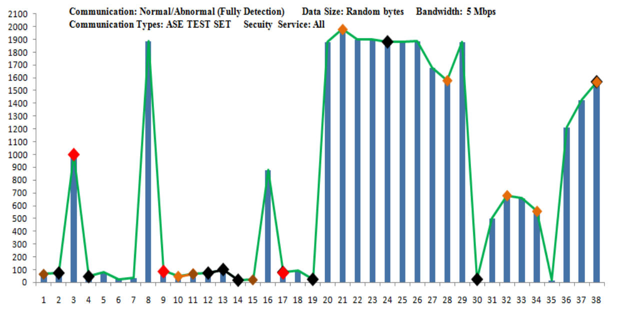
SCIN	Solution^{1}: Bytes Encryption	Solution^{2}: Key Encryption	Security
Directory 1	Sept 1: Bytes encryption using AES algorithms	Sept 1: AES key appended with bytes	Authentication, Confidentiality
	Sept 2: Sept 1; hash digest using SHA-2 algorithm.		Integrity
	Sept 3: Sept 2; encryption using RSA algorithm		Digital Signature /Non repudiation
	Sept 4: Sept 1 and Sept 3; public key encryption using RSA algorithm		Authentication, Confidentiality
Directory 2	Setp5: Uses private key (R) and public key (S) for decryption. The hash digest value and AES key formed.		Authentication, Confidentiality, Non repudiation
	Sept 6: Generate hash digest and match with sender (S) hash value.		Integrity
	Step 7: Use AES key to open and un-appended (case of Method^{2}) the bytes.		Authentication, Confidentiality

TABLE 2. Testbed Experiments: Level of Attack Detection

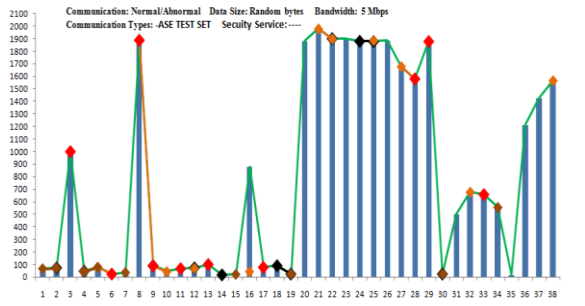
Testbed Experiment No	With Security Solution : SCADA Simulation (ASE Testset; Test Harness) Successful (S)/Non-Successful(N)				Without Security Solution : SCADA Simulation (ASE Testset; Test Harness) Successful (S)/Unsuccessful(U)			
	A. Attack	C. Attack	I. Attack	R. Attack	A. Attack	C. Attack	I. Attack	R. Attack
1	(N;N)	(N; S)	(N;S)	(S; S)	(S;S)	(S;S)	(S;S)	(S;S)
2	(N;S)	(S;N)	(N;N)	(S;S)	(S;S)	(S;S)	(S;S)	(S;S)
3	(S;N)	(N;S)	(N;S)	(N;N)	(S;S)	(S;S)	(S;S)	(S;S)
4	(N;N)	(S;N)	(N; S)	(S; S)	(S;S)	(S;S)	(S;S)	(S;S)
5	(S;N)	(N;N)	(N;N)	(S;N)	(S;S)	(S;N)	(S;S)	(S;S)
6	(N; S)	(N;N)	(N; S)	(N;S)	(S;S)	(N;S)	(S;S)	(S;S)
7	(N;N)	(N;N)	(S;S)	(S;N)	(S;N)	(S;S)	(S;S)	(S;S)
8	(S;S)	(N;N)	(N;N)	(N;N)	(S;S)	(N;S)	(S;S)	(S;S)
9	(S; S)	(N;N)	(N; S)	(N; S)	(S;S)	(S;S)	(S;S)	(S;S)
10	(N; S)	(N;N)	(S; S)	(N; S)	(S;N)	(S;S)	(S;S)	(S;S)
11	(N;N)	(N; S)	(S;N)	(S;N)	(S;N)	(S;S)	(S;S)	(S;S)
12	(N; S)	(S;N)	(N;N)	(N;N)	(N;S)	(S;N)	(S;S)	(S;S)
13	(N;N)	(S; S)	(N;N)	(S; S)	(S;S)	(S;S)	(S;S)	(S;S)
14	(N;N)	(S;N)	(N;S)	(N;N)	(S;S)	(S;S)	(S;S)	(S;S)
15	(N;S)	(N;N)	(N;N)	(S;N)	(S;S)	(S;N)	(S;S)	(S;S)
16	(S; S)	(S;N)	(N; S)	(S; S)	(S;S)	(S;S)	(N;S)	(S;S)
17	(S; S)	(S;N)	(N;N)	(N;N)	(S;S)	(S;S)	(S;S)	(S;S)
18	(N;N)	(N;N)	(N;N)	(N;N)	(S;S)	(S;S)	(S;N)	(S;S)
19	(N; S)	(S;S)	(N;N)	(S; S)	(S;S)	(S;S)	(S;S)	(S;S)
20	(N; S)	(N; S)	(N; S)	(N;N)	(S;S)	(S;S)	(S;S)	(S;S)
21	(N;N)	(N;N)	(S;S)	(S;N)	(S;S)	(S;S)	(N;S)	(S;S)
22	(S;S)	(N; S)	(N;N)	(N; S)	(S;S)	(S;N)	(S;S)	(S;S)
23	(N; S)	(N;N)	(N;N)	(N;N)	(S;S)	(S;S)	(S;S)	(S;S)
24	(N; S)	(S;N)	(N; S)	(N; S)	(S;S)	(S;S)	(S;S)	(S;S)
25	(N;N)	(S;N)	(S;N)	(S;N)	(S;S)	(S;S)	(S;S)	(S;S)
26	(S;N)	(N; S)	(N;N)	(S; S)	(S;S)	(S;S)	(S;S)	(S;S)
27	(N;N)	(S;N)	(N;S)	(N;N)	(S;S)	(S;S)	(N;S)	(S;S)
28	(N; S)	(N;N)	(S; S)	(N; S)	(S;S)	(S;S)	(S;S)	(S;S)
29	(S;S)	(S;N)	(N;N)	(S;N)	(S;S)	(S;S)	(S;S)	(S;S)
30	(N;N)	(S;N)	(N;N)	(N;N)	(S;S)	(S;S)	(S;S)	(S;S)
31	(S;N)	(N;N)	(S;N)	(S; S)	(S;S)	(S;S)	(S;S)	(S;S)
32	(N;N)	(N;N)	(S;N)	(N;N)	(S;S)	(S;S)	(S;S)	(S;S)
33	(N;N)	(S;S)	(N;N)	(S;N)	(N;S)	(S;S)	(S;S)	(S;S)
34	(S;N)	(S;N)	(S;N)	(N;N)	(S;S)	(S;S)	(S;S)	(S;S)
35	(N;N)	(N;N)	(N;N)	(N; S)	(S;S)	(S;S)	(S;S)	(S;S)
36	(S;N)	(N;N)	(S;N)	(S;N)	(S;S)	(N;S)	(S;S)	(S;S)
37	(S; S)	(N;S)	(S;N)	(S; S)	(S;S)	(S;S)	(S;S)	(S;S)
38	(N;S)	(S;N)	(S;N)	(N;N)	(S;S)	(S;S)	(S;S)	(S;S)

TABLE 3. Level of Attack Detection with/without Security Implementation

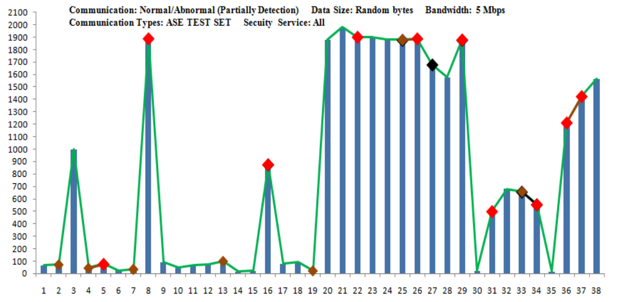
Security Tests	Successful (Times)		Successful (Times)	
	Test Harness		ASE Testset	
Communication	**End-to-End**	**Without**	**End-to-End**	**Without**
Authentication Attacks	6	20	3	10
Confidentiality Attacks	4	20	10	11
Integrity Attacks	6	21	7	15
Non-Repudiation Attacks	2	19	3	10
Total :	**18**	**80**	**23**	**46**
Partially : Attacks Detection	**40**	**64**	**36**	**98**



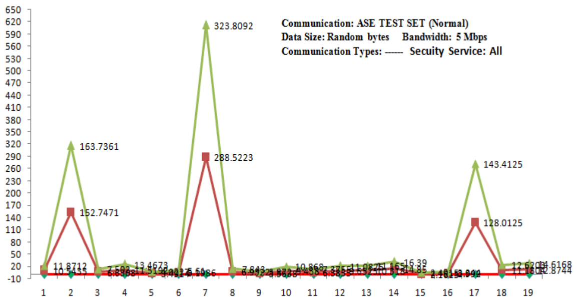
Graph1. ASE Testset: Abnormal Communication (With Security, fully detection)



Graph 2. ASE Testset: Abnormal Communication (Without Security)



Graph 3. ASE Testset: Abnormal Communication (With Security, partially detection)



Graph 4. ASE Testset: Latency Using Solution ^{1}and Solution^2

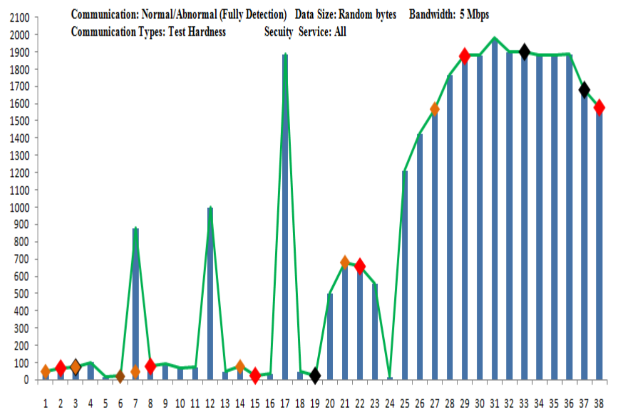
Blue line/Red Line	Dark Green Line/Light Green Line	Red /Black Marker	Orange /Brown Marker	X-axis	Y-axis
Testbed: Communication/ Latency Using Solution^2	Communication Ratio: Successful/ Latency Using Solution^1	Attacks: Authentication/ Confidentiality	Attacks: Integrity/non-Repudiation	No. of Successful Experiments	Bytes Utilization

TABLE 4. Performance Results via Security Implementation

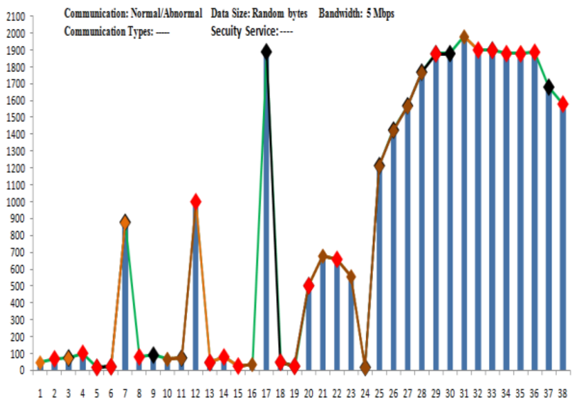
Results (Performance)	End-to-End(Test Harness)		End-to-End (ASE Testset)	
	Counted (%)	**Original (%)**	**Counted (%)**	**Original (%)**
Attack Detection (%)	12%	11.84	15%	15.13
Attack Detection Unused (%)	26%	26.31	24%	23.68
Attack Impact (%)	30%	29.60/45 At	32%	31.57/48At
Security (%)	70%	70.04	68%	68.43

TABLE 5. Average Performance Results via Security Implementation

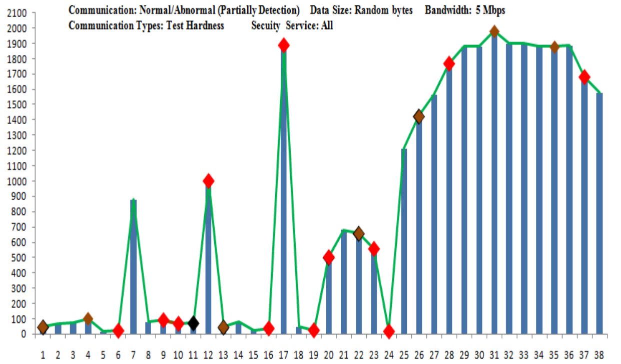
Final Results (Performance)	End-to-End (Test H)	End-to-End (ASE)	Average	Final
	Counted (%)	Counted (%)	Original (%)	Counted (%)
Attack Detection (%)				
Attack Detection Unused (%)	38	39	38.5	39%
Attack Impact (%)	30	32	31	31%
Security (%)	70	68	69	69%



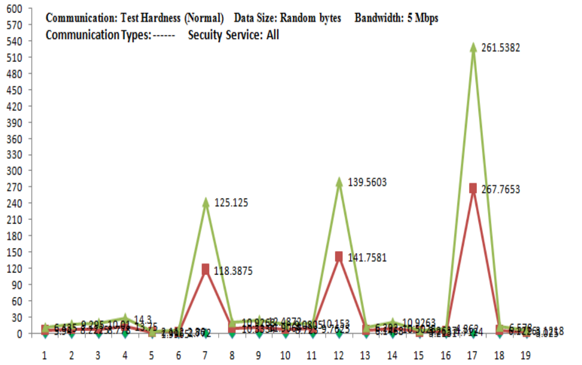
Graph 5. Test Harness: Abnormal Communication (With Security, fully detection)



Graph 6. Test Harness: Abnormal Communication (Without Security)



Graph 7. Test Harness: Abnormal Communication (With Security, partially detection)



Graph 8. Test Harness: Latency Using Method[1]and Method[2]

Blue line/Red Line	Dark Green Line/Light Green Line	Red /Black Marker	Orange /Brown Marker	X-axis	Y-axis
Testbed: Communication/ Latency Using Solution[2]	Communication Ratio: Successful/ Latency Using Solution[1]	Attacks: Authentication/ Confidentiality	Attacks: Integrity/non-Repudiation	No. of Successful Experiments	Bytes Utilization

]

TABLE 6. Performance Results without Security Implementation

Results (Performance)	Without(Testh)		Without(ASE)	
	Counted (%)	Original (%)	Counted (%)	Original (%)
Attack Detection (%)	53%	52.63	30%	30.26
Attack Detection Unused (%)	42%	42.1	64%	64.47
Attack Impact (%)	89%	89.47/136At	91%	90.78/138At
Security (%)	11%	10.53	9%	9.22

IV. CONCLUSION AND FUTURE WORK

Now days, the SCADA systems are connected with several proprietary and non- proprietary networks and allow transmission of data or bytes geographically, using transport protocols included TCP/IP with proprietary protocols over internet. This study has been deployed and established a secure communication link or channel designated as secure cryptography intermediate node (SCIN) between SCADA nodes. This study has anticipates the under lying concept that critical system or SCADA system are secure, while connecting with open networks or protocols or/and bytes transmission between proprietary and non- proprietary protocols. At other side, the current study also anticipated; the uses of security mechanisms and more advance cryptography solutions, which provide accurate performance and independency without limitations against SCADA security.

In future work, the proprietary protocols as a part of SCADA system security issues will analyze and generic prototype will design and deploy against security issues, while connecting with non proprietary protocols/network.

REFERENCES

[1] Shahzad, S., A. Aborujilah and M. Irfan, “A New Cloud Based Supervisory Control and Data Acquisition Implementation To Enhance The Level 0f Security Using Testbed,” 2014, DOI: 10.3844/jcssp.2014.652.659

[2] S. Musa, A. Shahzad and A.Aborujilah, “Secure security model implementation for security services and related attacks base on end-to-end, application layer and data link layer security,” Proceeding ICUIMC '13 Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, 2013, DOI: 10.1145/2448556.2448588

[3] S. Musa, A. Shahzad and A.Aborujilah,”Simulation base implementation for placement of security services in real time environment,” Proceeding ICUIMC '13 Proceedings of the 7th International Conference on Ubiquitous Information, 2013, DOI: 10.1145/2448556.2448587

[4] Martin Drahansky; Maricel Balitanas, “Cipher for Internet-based Supervisory Control and Data Acquisition Architecture,” Journal of Security Engineering, 2011

[5] Shahzad, S. Musa, A.Aborujilah, M.N.Ismail and M.Irfan, “Conceptual Model of Real Time Infrastructure within Cloud Computing Environment,” International Journal of Computer Networks (IJCN), Volume (5): Issue (1), 2013.

[6] Rosslin John Robles; Maricel Balitanas; Tai-hoon Kim, “Security Encryption Schemes for Internet SCADA: Comparison of the Solutions,” Communications in Computer and Information Science, Volume 223, 2011, pp 19-27, DOI: 10.1007/978-3-642-23948-9_4

[7] Applied Systems Engineering, Inc., “ASE2000 Communication Test Set Version 2 User Guide,” Document Revision 1, 2011.

[8] Triangle Microworks, Inc., “Communication Protocol Test Harness Product Documentation,” Version 3.15, 2013.

[9] Kiuchi, M. Serizawa,and Yoshizumi, “Security technologies, usage and guidelines in SCADA system networks,” ICCAS-SICE, IEEE, 2009.

[10] James H. G. Sandip, C. Patel, “Security Considerations in SCADA Communication Protocols,” Intelligent Systems Research Laboratory Technical Report.

[11] J. Moteff and P.Parfomak, “Critical Infrastructure and Key Assets:Definition and Identification,” Resources, Science, and Industry Division, CRS Report for Congress, 2004.

[12] Yongge Wang,“Chapter1:Smart Grid, Automation, and SCADA Systems Security,” World Scientific Review Volume, 2012.

[13] D. Dolezilek, K. Carson, K. Leech, and K. Streett, “Secure scada and engineering access Communications: a case study of private and Public communication link security,” Schweitzer Engineering Laboratories, Inc. Pullman, Washington USA,2003.

[14] Shahzad, S., A. Aborujilah, M. Irfan, Secure Cryptography Testbed Implementation for SCADA Protocols Security, ACSAT 2013, IEEE, DOI: 10.1109/ACSAT.2013.69

[15] Shahzad, S., A. Aborujilah, M. Irfan, Industrial Control Systems (ICSs) Vulnerabilities analysis and SCADA Security Enhancement Using Testbed Encryption, ICUIMC, ACM, 2014, DOI: 10.1145/2557977.2558061

[16] Shahzad, S., A. Aborujilah, M. Irfan, A Performance Approach: SCADA System Implementation within Cloud Computing Environment, ACSAT 2013, IEEE, DOI: 10.1109/ACSAT.2013.61

[17] Chen Yuan; Dong Qingkuan, “RCCA security for KEM+DEM style hybrid encryptions and a general hybrid paradigm from RCCA-secure KEMs to CCA-secure encryptions,” Security Comm. Networks, 2014, 7, 1219–1231, DOI: 10.1002/sec.853

[18] Shahzad, S., M. Irfan, N-Secure Cryptography Solution for SCADA Security Enhancement, Trends in Applied Sciences Research, 2014, DOI: 10.3923/tasr.2014.381.395

[19] Shahzad, S., M. Irfan, Key Encryption Method for SCADA Security Enhancement, Journal of Applied Sciences ,2014, DOI: 10.3923/jas.2014.2498.2506

[20] Fujisaki E; Okamoto T., “Secure integration of asymmetric and symmetric metric encryption schemes,” In Advances in Cryptology – CRYPTO'99, LNCS, Vol. 1666. Spring-Verlag, 1999, pp.537–55