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