Journal of Computer Science 10 (4): 652-659, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.652.659 Published Online 10 (4) 2014 (http://www.thescipub.com/jcs.toc)

A NEW CLOUD BASED SUPERVISORY CONTROL AND DATA ACQUISITION IMPLEMENTATION TO ENHANCE THE LEVEL OF SECURITY USING TESTBED

[1]A. Shahzad, [1]S. Musa, [1]A. Aborujilah and [2]M. Irfan

[1]Malaysian Institute of Information Technology (MIIT), University Kuala Lumpur, Malaysia
[2]Windfield College, Kuala Lumpur, Malaysia

Received 2013-10-17; Revised 2013-12-19; Accepted 2013-12-21

ABSTRACT

Now days cloud computing is an important and hot topic in arena of information technology and computer system. Several companies and educational institutes have been deployed cloud infrastructures to overcome their problems such as easy data access, software updates with minimal cost, large or unlimited storage, efficient cost factor, backup storage and disaster recovery and several other benefits compare with the traditional network infrastructures. In this research paper; Supervisory Control and Data Acquisition (SCADA) system has been deployed within cloud computing environment, to minimized the cost (that are related with real time infrastructure or SCADA implementation) and take the advantages of cloud computing. The command bytes (data) have been transmitted between SCADA nodes and traffic is monitored and controlled simultaneously at master (main controller) site. During communication, security is a major issue because usually, SCADA system and cloud infrastructure had been deployed without any security consideration. In current testbed implementation, strong security mechanism (using cryptography solution) has been deployed, while exchanging commands within cloud environment (SCADA within cloud environment). Several times attacks included "authentication, integrity, confidentiality and non-repudiation" have been lunched, to evaluate the security solution (proposed security solution) and security during abnormal communication.

Keywords: Cloud Infrastructure, Supervisory Control and Data Acquisition (SCADA) System, Security Issues, Virtual Environment

1. INTRODUCTION

The cloud infrastructure is a treasure of resources that provides services according to the requirements of user or for business activities. Now days, cloud computing technology is increasing rapidly, over the world due to the needs of users (subscribers) and business prospective (companies' requirements). Cloud computing is similar as distribution communication architecture, where applications or services are accessed by several users at same time. Large number of users (within virtual environment) is accessing their acquired resources from cloud server (from control center) simultaneously, via internet (Breiter, 2010). The applications and resources are allocated at central controller (cloud server) and cloud users (subscribers) or other connect nodes accessing their applications or software without installation on local machines with minimal cost. Programs and applications are running simultaneously within several connected machines (user sites), with efficient processing during communication. Cloud infrastructure provides centralized repository, where each connected user can store data files and access their files and information upon needs (user needs). As conclusion, cloud computing infrastructure provides lager number of resources and applications to their users (connected users) without any installation at user machine and efficient storage space (repository) that could be helpful during disaster recovery. Mean that, in the case of data

Corresponding Author: A. Shahzad, Malaysian Institute of Information Technology (MIIT), University Kuala Lumpur, Malaysia

or information loosed, then will recovery from cloud repository (centralized repository).

The cloud computing infrastructure provides basic three types of services for their users (subscribers) or business processing (activities) included "Software as a service or SaaS (Users can access on demand applications such as databases and other software), Platform as a service or PaaS (users are able to used operating systems and other platforms such as programming tools to developed their applications and executed without purchasing any expense application environment), Infrastructure as a service or IaaS (users are able to use physical infrastructures as virtual machine, monitor by hypervisor) and other services included Hardware as a Service or HaaS, everything as a Service EaaS and Network as a Service (NaaS)". Cloud computing has number of benefits, while deploying these services included "easy access to application and other resources, fast development and execution, centralized unlimited storage, automatic integration, storage and disaster recovery, minimized session and infrastructure risks, cost less solution, research innovations, scalability, availability, reliability, enhance accessibility and flexibility and efficiency (as whole), (Sun, 2009; Badger *et al*., 2011).

Supervisory Control and Data Acquisition (SCADA) systems are parts of Industrial control system or ICS, which have been widely deployed in real time infrastructures such as electrical houses, water treatment plants, oil refinery industries and gas stations. SCADA systems have prominent place in industries (real time industries), due its services. SCADA system provides central controller to control and monitor whole (industries communication) communication via internet. SCADA processes are distributed at several remote sites and master controller is used to control the overall communication. In SCADA architecture, remotes stations (client nodes) are directly connected with physical environments using Light-Emitting Diodes (LEDs), sensors and programmable logic controllers or PLCs and processing information (real time information) to master station. The master controller (master station) is superior within SCADA network that control and send request commands to remote station and then remote node executes (generates) the request and send response back to master station (according to master request). Typically, commands are read/write functions, alarm at abnormal condition, master polling (integrity and event) and others. The historian is deployed within SCADA system, that is used to store and access data or information based on events or acquirements of master/remote stations. With the growing demands of Industrial Control Systems (ICSs) and advance I.T infrastructure, SCADA systems are also connected with several open networks such as LAN (wire/wireless) and WAN (wire/wireless). Using modern I.T infrastructure, SCADA system applications are distributed at several remote locations (remote fields) and have monitored at controller center via internet. Now days, SCADA system also uses non-proprietary protocols included DNP3, Modbus and Fieldbus, rather than proprietary protocols, which significantly enhanced the performance of SCADA communication (Stouffe and Scarfone, 2011).

2. LITERATURE SURVEY

The two solutions have been suggested to deploy SCADA system within cloud computing environment that significantly minimized the cost and enhance reliability and scalability. Several cloud based infrastructures have been deployed all over the world in various sectors included industrial and educational sectors. The cloud technology is relatively new for SCADA system communication. By deploying SCADA system within cloud computing environment, its can minimized the expense and provides lager number of resources on user demands (real time industrial demands) (Mishra *et al*., 2013). The two solutions have been suggested to deploy the SCADA communication within cloud computing environment. In first solution, SCADA system (network) has been located separately and cloud infrastructure is used for storage and visualization purposes. In second solution, SCADA system (applications) has been entirely deployed within cloud computing environment and fields devices communicate with each other via cloud (Shahzad *et al*., 2013; InduSoft, 2012).

The detail review has been conducted based on cloud and SCADA system (cloud network) security issues and cryptography solutions have been implemented to secure the SCADA communication, while connected with open standard networks and protocols. During communication, encrypted message (bytes) has been transmitted between master/remote nodes and results are measured. The performance results within abnormal communication, concludes that the security has been significantly enhanced by deploying encryption security solutions within SCADA communication (Shahzad *et al*., 2013). In this research, security has been also tested within SCADA wireless communication and results are measured to validate the security solution (encryption solution) (Musa and Aborujilah, 2013a).

3. PROBLEM STATEMENT

SCADA system has number of benefits included manageability, reliability and more scalability during

communication, while deploying within cloud computing environment. At other side, this advance implementation has number of security issues and challenges, which warms the communication of real time infrastructures or industries. In cloud environment, SCADA applications are distributed at several locations using open networks and protocols via internet. The large SCADA system connectivity with non-proprietary networks and protocols, significantly effect the communication of real times infrastructures. Several solutions have been also suggested and deployed to minimize the security issues of SCADA system using firewall protection, intrusion detection and prevention system and DMZ. These solutions provide limited security against attacks. So, a security solution is needs that has resistance to overcome the security issues and provide more protection for SCADA system against attacks/threads (Shahzad *et al*., 2013; InduSoft, 2012).

Based on current cloud and SCADA system security issues, several security solutions have been proposed and implemented included using SSL, TLS, IPsec and other security solutions. Buts all these solutions provide limited security for SCADA (SCADA-Cloud system) communication and mostly, are relies on other security protocols such as digest signature and cryptography algorithms (Abu-Ein *et al*., 2012). In this research, the detail survey has been conducted that is based on SCADA (SCADA-Cloud system) system security issues and its major vulnerabilities and cryptography solution has been proposed to secure the SCADA (SCADA-Cloud system) communication (Shahzad *et al*., 2013).

4. SCADA_CLOUD ARCHITECTURE

SCADA master control application such as human machine interface has been installed within cloud computing environment and stations (virtual nodes) are allow to access data/information from centralized repository called historian. Mean that data or commands are requested from master station via cloud and remote station generates the response and send back to master station also via cloud. The virtual machines (nodes) sharing the repository (using tool: MySql) that has been entirely located within cloud environment. During communication, information has been visualized at each node and simultaneously stored within repository. The historian is also used for creating backups and reporting purposes, while acquired by master/remote nodes or based on events occurs (Liu *et al*., 2011; Shahzad *et al*., 2013; Siemens, 2010).

In **Fig. 1**, SCADA field devices are connected with master station or master node via cloud. Within communication network (Cloud_SCADA system), the master/remote stations have been connected with user interface, directly access from cloud. During communication, information has been stored within historian that also located in cloud environment and each node can access and performs its queries to/from the historian (Shahzad *et al*., 2013; Musa and Aborujilah, 2013b).

5. SETUP AND CONFIGURATION

In testbed setup, six remote nodes (virtual nodes: VRTU1, VRTU2, VRTU3, VRTU4, VRTU5 and VRTU6) have been connected with master node (virtual node: VMTU) within cloud computing environment and access the resources included database (historian), user access interface and communication visualization, directly from cloud. Each time, master node has initialized the communication and remote nodes that are directly connected with physical environment, generate the commands and send back the response, based on master request. Several times data/information has been transmitted from master station to remote stations and remote stations to master station via cloud and performance results (based on normal and abnormal communication) are measured with the bandwidth of 5 Mbps. **Figure 2** illustrates the SCADA_Cloud testbed communication setup.

6. TESTBED IMPLEMENTATION

Master node (virtual node: VMTU) is superior within testbed communication, mean that only master node is authorized to initial the communication with connected remote nodes (virtual nodes) via cloud. Each time, master initialized and sends the request message or command (execution) to remote station, the message or bytes are encrypted with secret key, using AES algorithm. The requested bytes hash digest has been calculated to protect the SCADA communication from integrity attacks, using SHA-2 hashing algorithm. Hashing values are calculated at both ends (master and remote station), to conclude that message (bytes) have been transmitted securely and contents are not changed during communication. The private key is used to encrypt the hash digest value that has been calculated from SHA-2 algorithm. This encryption process uses as digital signature, to verify the non-repudiation security against attacks. At the end, secret key and encrypted hash digest is again encrypted with public, using RSA algorithm.

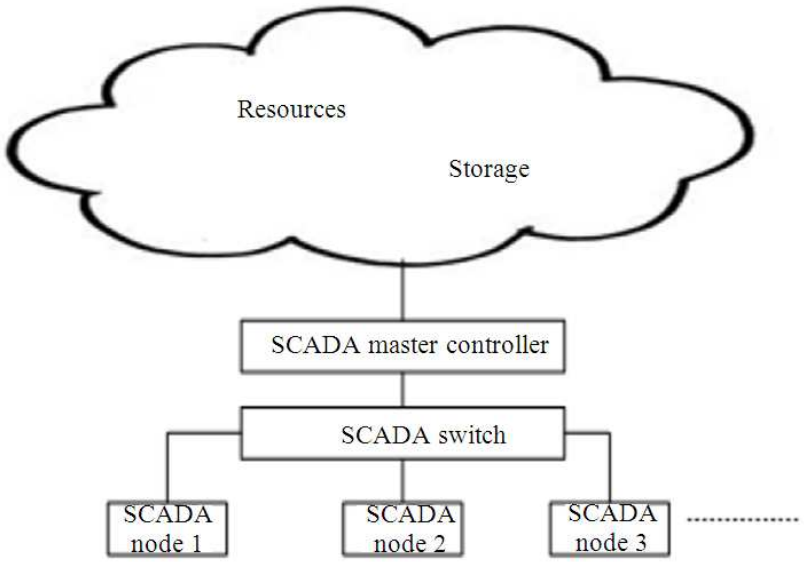

Fig. 1. SCADA_Cloud architecture

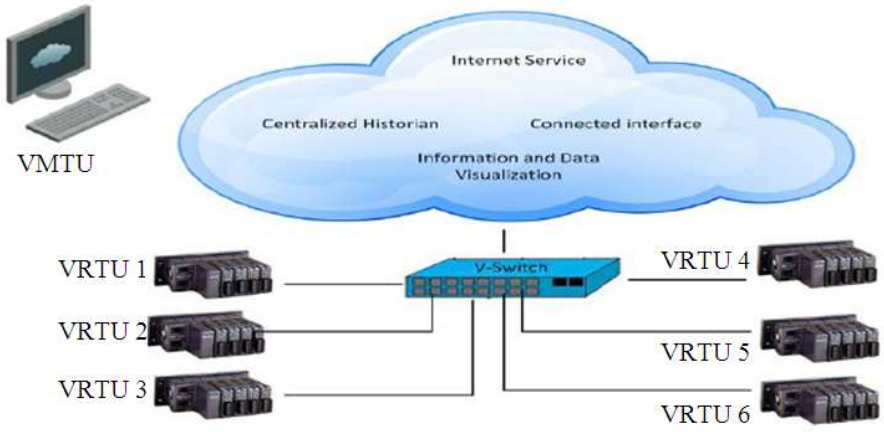

Fig. 2. SCADA_Cloud testbed setup

Upon receiving message (bytes), remote station uses its private key and master public key to decrypt the secret key and hash digest. This process (decryption) also verifies the communication against non-repudiation attacks. The secret key is used to decrypts the message and verifies the communication against authentication, confidentiality attacks. The hash value has calculated at remote site and compared with master node hash value (digest) to verify the integrity attacks (Musa and Aborujilah, 2013a).

Sender Site (Proof)

Suppose is $\mu_{S(m,b,E[k])}$ bytes information (bytes), uses within testbed for the purpose of security (security implementation). Such that Equation (1):

$$\sum \mu_{S(m,b,E[k])} \ldots\ldots \tag{1}$$

$$\varepsilon\, b \in B \Lambda k \in K \underset{Eny}{\Leftrightarrow} \exists : \forall \mu_{S(m,b,E[k])} : M1.Sym^{f} Eny \underset{E \to Sym^{b}}{i \leftarrow u_{rb}} \tag{2}$$

$$E\left[SC_{S}^{k}\left\{\sum \mu_{S(m,b,E[k])}\right\}\right] \in M \ldots\ldots$$

Equation (2) shows the encryption process using symmetric algorithm:

$$M2.Aym^{f}(H^{f})Eny\ i \underset{\substack{E\rightarrow Aym^{f}\\ H\rightarrow H^{f}}}{\leftarrow} u_{rb} \quad E\left[Pr_{S}^{k}\left\{H\left(\sum \mu_{S(m,b,E[k])}\right)\right\}\right] \in M\ldots\ldots \tag{3}$$

Equation (3) shows the encryption process using asymmetric and hashing algorithms:

$$M3.Aym^{f}Eny\ i \underset{E\rightarrow Aym^{f}}{\leftarrow} u_{rb}\ E\left[PU_{R}^{k}\{M1,M2\}\right] \in M \vee M1 \wedge M2 \wedge M3 \in M\ldots\ldots \tag{4}$$

Equation (4) shows the encryption process using asymmetric algorithm and message 'M' represents the total payload transmitted from MTU to RTU.

Receiver Site (Proof):

Suppose message 'M' has been received at receiver site or RTU. Such that:

$$D(M) == D\begin{bmatrix} M3.Aym^{f}\ \ Eny\ i \underset{E\rightarrow Aym^{f}}{\leftarrow} u_{rb} \\ E\left[PU_{R}^{k}\{M1,M2\}\right] \end{bmatrix} \Rightarrow M.Aym^{f}\ Dny\ i \underset{E\rightarrow Aym^{f}}{\leftarrow} u_{rb}\ D\left[Pr_{R}^{k},Pu_{S}^{k}\{M3\}\right]\ldots\ldots \tag{5}$$

Equation (5) shows the decryption process using asymmetric algorithm:

$$M.Sym^{f}\ Dny\ i \underset{E\rightarrow Sym^{f}}{\leftarrow} u_{rb}\ D\left[Sc_{R}^{k}\{M1\}\right]\ldots\ldots \tag{6}$$

Equation (6) shows the decryption process using symmetric algorithm:

$$H\left(\sum \mu_{S(m,b,E[k])}\right) \in h_{digest^{R}}\ldots\ldots \tag{7}$$

In Equation (7), the hash digest (receiver site) has been calculated and comparison operation will perform with sender hash value:

$Comp^{H}.H\left[h_{digest^{R}}, h_{digest^{S}}\right] \Rightarrow h_{digest^{R}} == h_{digest^{S}}$, equal hahs values and $h_{digest^{S}}, h_{digest^{S}} \in H$

During communication, cryptography keys are kept secure within historian and each node has been configured with secure channel. Several times, testbed have been run and security performances are measured against intruders. Abnormal traffic has been created between master node to cloud and remote node to cloud and performances are measured and compared (Musa and Aborujilah, 2013b). In security performance **Fig. 3 and 4**, the attacks detection (%) and attacks impact (%) ratio on system between abnormal (with proposed solution) and abnormal (without proposed solution) communication (testbed) is comparatively high during master node accessing the resources of cloud, while comparing with proposed implementation performance results.

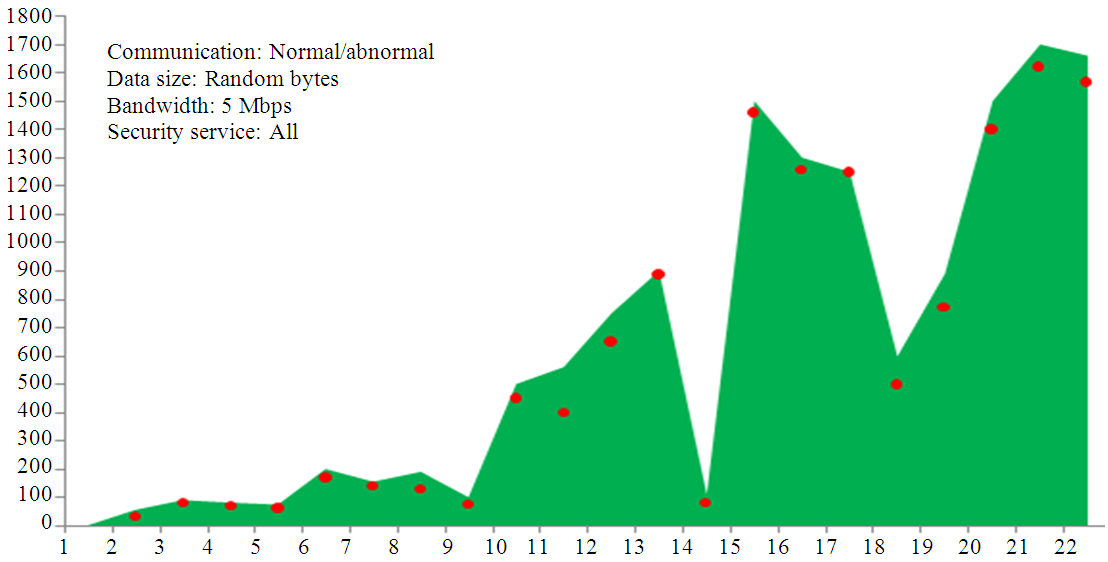

Fig. 3. Abnormal communication without proposed solution (Master site)

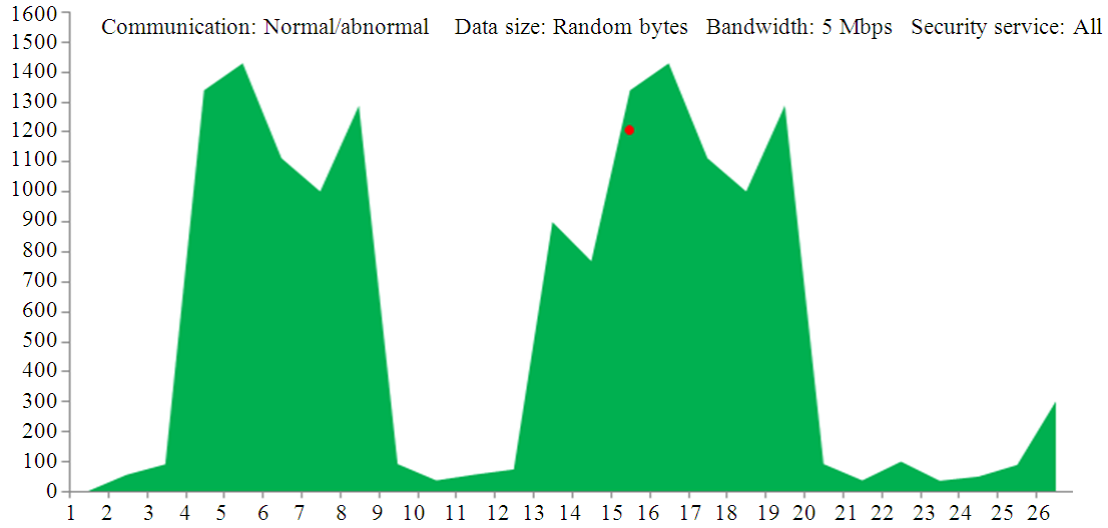

Fig. 4. Abnormal Communication with Proposed Solution (master site)

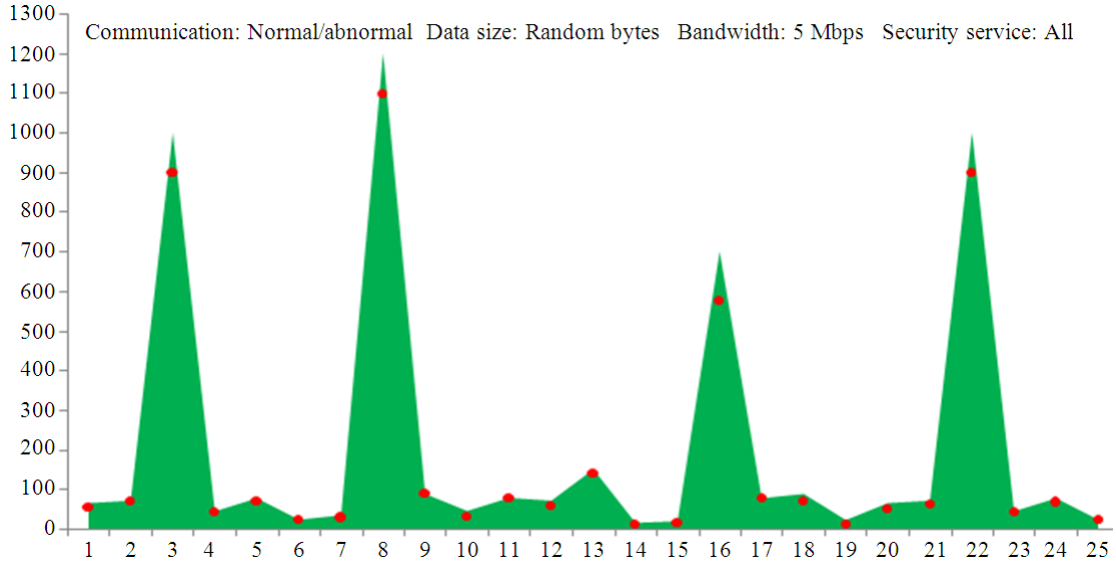

Fig. 5. Abnormal Communication without Proposed Solution (Remote Site)

The proposed implementation successfully achieves the security paradigms included authentication, integrity, confidentiality and non-repudiation, during testbed communication.

In security performance **Fig. 5 and 6**, the security level has been also measured during remote node accessing the resources of cloud and performance measurements included attacks detection (%) and attacks impact (%) ratio on system (testbed) is also compared between with/without proposed implementation.

The proposed implementation successfully achieves the security paradigms include authentication, integrity, confidentiality and non-repudiation, during testbed communication. **Table 1** shows the overall level of security during testbed communication (with and without proposed solution).

In performance **Fig. 3-6**, the green flow lines show the communication with different data rates, while red dots (markers) represent the level of attacks during communication.

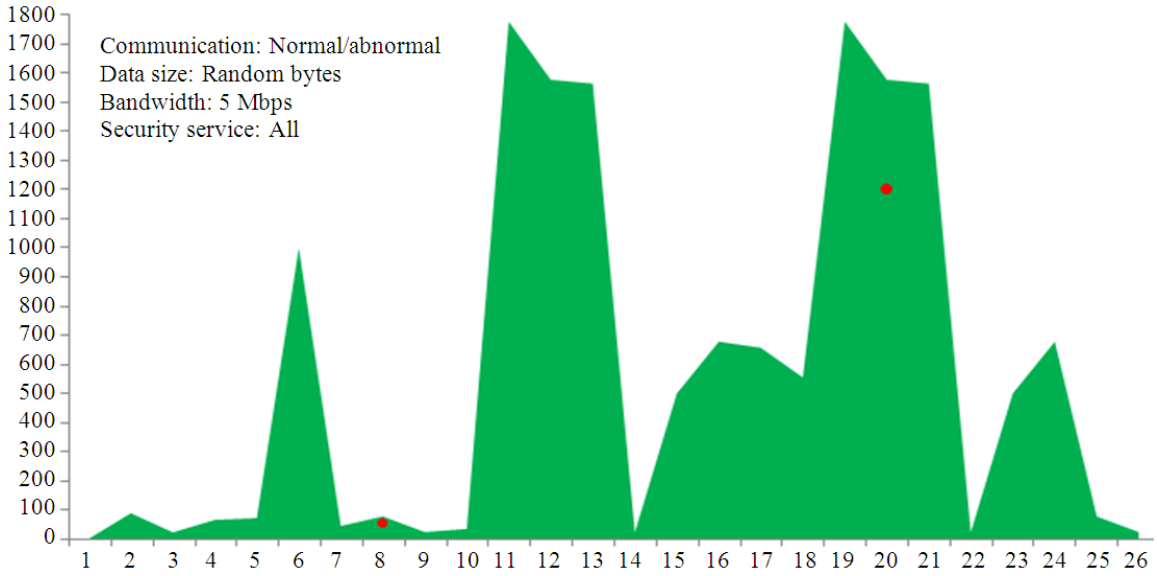

Fig. 6. Abnormal Communication with Proposed Solution (Remote Site)

Table 1. Performance comparison with/without proposed solution

	Abnormal: SCADA_Cloud communication with proposed implementation		Abnormal: SCADA_Cloud communication without proposed implementation	
Attacks	Attack detection (%)	Attack impact (%)	Attack detection (%)	Attack impact (%)
Guessing shared key	App. 2	App. 1	App. 91	App. 90
Brute force	App. 3	App. 1	App. 91	App. 91
Password guessing	App. 5	App. 1	App. 95	App. 93
Frame/bytes injection	App. 7	App. 0	App. 92	App. 92
Data replay	App. 8	App. 2	App. 95	App. 93
Data deletion	App. 9	App. 2	App. 94	App. 93
Eavesdropping	App. 2	App. 0	App. 96	App. 97
Key cracking	App. 1	App. 0	App. 97	App. 97
Man-in-the-middle	App. 3	App. 0	App. 96	App. 96

Results are written withour any decimal point and app. Is stand for approximately value

7. SOLUTION COMPARISON

The SCADA system deployment within cloud computing environment is new approach to minimize the cost factor and achieve more reliability and scalability. Few organizations included “Microsoft, Sabre Industries, IBM, InduSoft, Trend Micro and other” have implementation which is based on SCADA within cloud environment, but the security is an important issue during communication. Few researches have also proposed security implementations included “Secure Shell (SSH), Internet Protocol Security (IPSec), Transport Layer Security (TLS)/Secure Sockets Layer (SSL)”, but these solutions have also limitation (unable to perform non-repudiation function) and mostly are based on digital signature and other cryptograph solutions.

8. CONCLUSION

The cloud computing platform is a most reliable and cost less solution for real time infrastructures such as Supervisory Control and Data Acquisition (SCADA) systems and other Industrial Control Systems (ICSs). In current research, SCADA system has been deployed within cloud environment, to minimize the implementation cost and achieve more benefits during communication. A cryptography solution has been implemented successfully during testbed communication

(commands or bytes exchanging) and results are measured during abnormal communication, while deploying with/without proposed security (cryptography) solution. The performance measurements conclude that, the proposed cryptography solution successfully enhanced the testbed (SCADA within cloud environment) security during abnormal communication.

9. REFERENCES

Abu-Ein, A.A.K., H.M.S. Hatamleh, A.A.M Sharadqeh, A.M. Alnaser and O. AlHeyasat, 2012. E-commerce: Security and applications. Am. J. Applied Sci., 9: 1868-1871. DOI: 10.3844/ajassp.2012.1868.1871

Badger, T., R. Corner and J. Voas, 2011. Draft cloud computing synopsis and recommendations. Recommendations of the National Institute of Standards and Technology.

Breiter, I.B.M., 2010. Cloud computing architecture and strategy.

InduSoft, 2012. Cloud-based SCADA system for the Oil and Gas industry.

Liu, J., J. Mao, R. Bohn, J. Messina and L. Badger *et al*., 2011. NIST cloud computing reference architecture. NIST Special Publication 500-292.

Mishra, R., S. Jain and J.S. Rathore, 2013. Cloud computing security. Int. J. Recent Innov. Trends Comput. Commun.

Musa, A.S. and A. Aborujilah, 2013b. Secure security model implementation for security services and related attacks base on end-to-end, application layer and data link layer security. Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, (MC' 13).

Musa, A.S. and A. Aborujilah, 2013a. Simulation base implementation for placement of security services in real time environment. Proceedings of the 7th International Conference on Ubiquitous Information, (UN' 13), ACM Press, New York, USA.

Shahzad, S., A. Aborujilah, M.N. Ismail and M. Irfan, 2013. Conceptual model of real time infrastructure within cloud computing environment. Int. J. Comput. Networks.

Siemens, A.G., 2010. Cloud computing architecture. Proceedigns of the 4th Generation Datacenter IEEE Spectrum, (IS' 10).

Stouffe, J.F. and K. Scarfone, 2011. Guide to Industrial Control Systems (ICS) Security. NIST Special Publication.

Sun, M., 2009. Introduction to Cloud Computing Architecture. 1st Edn., White Paper.