

# New Modeling Approach: To Enhance the Networks Performance Based on Communication Issues and Related Security

AAmir Shahzad, Malrey Lee, Kim Geon, Muhammad Irfan

**Abstract**— The new technology demands and rapid utilization of Information technology (IT) have been increasing day by day, in all over the world. The growing demands of advance Information technology (IT) infrastructures within several Industries and organizations, and the implementation of non-propriety protocols with propriety protocols, caused major performance issues in the terms of communication, data exchange and security.

In this proposal, detail survey has been conducted that is based on several computer or/and Information technology (IT) networks deployment with their security requirements and issues. The proposed research thoroughly study the implementations related with communication networks included local area network (LAN) and wide area network (WAN) as part of traditional networks, mobile networks, real time networks and cloud computing networks. Also study the existing Implementations of common protocols that have been used during communication (network communication).

This research reviews the exiting implementations related with propriety and non-propriety protocols within networks infrastructures with security implementations. After reviewed the exiting work or implementations in detail, this research proposal proposed a generic model to overcome the communication issues, security weaknesses and proper implementation of security mechanisms with proper placement. The proposed model also tries to overcome the issues that have been situated between real time protocols and traditional protocols during communication.

**Keywords**— Traditional Networks; Real time Networks; Mobile Networks; Cloud Computing Infrastructure; Protocols.

## I. Introduction

The cloud computing is a concept the involved a larger number of networks or connected computers or nodes within networks which are configured together to sharing the resources and services. The cloud computing infrastructure is a reliable and chip or cost less way for sharing the resources/services in the terms of hardware and software,

between computers or nodes within network (LAN/WAN).The network architecture of cloud computing is same as distributed computing, where number of nodes are distributed at several locations and sharing the resources and services. The end-users can interact with their acquired applications and services via cloud server such as private or public, based on access permission and privileges. The end-users, industries and organizations are installing the numbers of software in their local computer system via cloud access and also allow for the hardware utilization virtually via cloud access, without any installation in local machine. This will save the cost included purchasing of expensive hardware and software. Usually, cloud resources are accessed by using four ways: “via private cloud, via public cloud, via community cloud and hybrid cloud,” and also provide services that are divided into three categories included “IaaS (cloud infrastructure as a service), PaaS (cloud platform as a service), and SaaS (cloud software as a service)” [4, 6].

The ICS (Industrial Control System) is designated for several types of critical infrastructure sectors included “SCADA (Supervisory Control and Data Acquisition) systems, DCSs (Distributed Control Systems), PLCs (Programmable Logic Controllers) and other controlling and monitoring systems”. Usually, real time systems have been designed to controller and monitor the assets that are located or distributed geographically at several locations. In past, the network design of these systems was limited and nodes are connected in limited area, or as standalone network. But the uses of advance information technology (IT), these systems are also moved from stand alone network to wide area network (WAN) or/and distributed network. The fast changed in technology (information technology), the system nodes are distributed at several locations via internet, and overall distributed or network architecture is controlling from the main server. The uses of internet technology or/and open networks and protocols such as TCP/IP and other, made the ICS (Industrial Control System) platform vulnerable form several types of thread and attacks, that causing major impact on the system performance included critical processing and automation [3, 5, 18].

In computer network; number of computers or nodes are connected together within local area network (LAN) or wide area network (WAN) for exchanging the data or bytes within specified network. The network nodes are connected together via media such as wire and wireless, for the purpose of exchanging the information. The mobile network is also a wireless network which is distributed geographically or at several locations, also designated as cell or cells. The cellular network is a faster way of

---

AAmir Shahzad, Malrey Lee  
1,2561-756,Center for Advanced Image and Information Technology,  
School of Electronics & Information Engineering,  
Chon Buk National University, 664-14, 1Ga, Deokjin-Dong,  
Jeonju, ChonBuk, Korea

Kim Geon  
Department of Records Management, Chon Buk National University,  
664-14, 1Ga, Deokjin-Dong, Jeonju, ChonBuk, Korea

Muhammad Irfan  
Infrastructure University Kuala Lumpur (IUKL), Malaysia

communication or information delivery in arena of information technology [1, 2, 19].

## II. Literature Review

Many larger organizations networks are distributed over the world for the purpose of information exchange and other. The distribution of applications and their access from remote sites or end-users access from remote locations, caused several performance issues or communication issues and most important one is security issue. The detail literature has been conducted based on the performances and security issues as part of organization operations and at the end, some countermeasures are highlighted to avoid the uncertain conditions and minimized the risks and issues that are related with performances during communication. Several common vulnerabilities have been discussed that are occurring during communication over internet included software or application insecurity, uses of malicious software, unauthorized nodes access in the terms of connection and privacy network or private network, internet DOS, unauthorized change in main controller or server, internet spoofing, and threads and attacks, which are warning the network communication [7, 8,12]. After conducting the detail vulnerabilities analysis, several countermeasures have been also highlighted included strong password uses during system/user or administrator login, installation of intrusion detection and prevention system, licensed and strong antivirus, monitoring software for change configuration detections, automated backup and recovery software, User/administrator awareness for handling and configuration during system disaster and uses security protection mechanism included firewall, DMZs and SSL/TLS [1, 14, 15, 16].

The real times systems such as SCADA systems and DCSs have been deploying the advance information technology infrastructures to enhance the performance and for system connectivity over the world via WAN. These systems networks or nodes are distributed at several locations at distance placed and all remotes nodes are connected with main node or main station via internet. These systems implementations are very important for industrial processing or automation included water pumping station, electricity controlling stations, and oil refining miles, etc. By deploying advance network infrastructure and connectivity between several propriety and non-propriety networks, caused major security issues during communication. So, generic solution or model has been acquired to resolve the issues or security issues which are linked with critical systems (real time systems). Many security solutions have been implemented to secure the communication of real times systems, but each solution has several limitations in the terms of implementation, dependences and performance [3, 5, 15].

Based on existing security implementations and their limitation within traditional networks, mobile networks, and real time networks, strong cryptography mechanism or solution has been implemented to secure these systems or networks communication. The cryptography solution using asymmetric and symmetric algorithms has been used to implement the security without any dependence or differ

from other security solutions [17]. The cryptography solutions have been proposed and successfully implemented to secure the ICS communication, while data or bytes transmitted for sender to receiver or vice versa. The main security objectives or security services included data (bytes) authentication, data (bytes) confidentiality, data (bytes) integrity and data (bytes) non-repudiation, have been implementation successfully and performance results are also measured during communication. Several attacks/threads have been launched to create the abnormal communication during transmission of bytes (data). The security performance results show that security mechanisms using cryptography have potential to secure the communication and data (bytes) are secure in abnormal communication. During transmission of bytes (data); the authentication security service has been successful implemented by RSA and AES algorithms as part of asymmetric and symmetric algorithms, the confidentiality security service has been successful implemented by RSA and AES algorithms as part of asymmetric and symmetric algorithms, the integrity security service has been successful implemented by SHA-1 and SHA-2 algorithms as part of hashing algorithm, and the non-repudiation security service has been successful implemented by digital signature algorithm [3, 5,12, 13,20,21,22,23,24].

Now days; cloud computing is a very famous topic or deployment in arena of information technology in all over the world. The cloud computing is a reliable and cost less solution for all deployment that are related with information technology or/and others. Several networks included traditional networks, mobile networks, and others, have been deployed within cloud computing infrastructure. Few researches have been also conducted to implement the real time systems such as SCADA system and DCSs systems within cloud computing infrastructure, but mostly deployments are conceptual based and have number of issues during implementation. The detail survey has been conducted which is based on the networks issues in the terms of performance and cost [9, 10, 11]. Based on review, a solution has been implemented or conceptually implemented to deploy the real time system in cloud computing environment. This research tries to implement the numbers of real system nodes that are located at distance placed and configured with main station. These remote nodes are controlled and monitor by cloud infrastructure. Each node or remote node has its own cloud infrastructure and connected with main cloud. The security is one of the important issues that suffer the communication, while data exchanging between nodes. The cryptography solution has been also proposed to secure the communication during cloud access [4, 6].

## III. Problem Statement

Now days, there is dramatic change found in information technology sectors in the terms of technology and connectivity. Number of network nodes is connected together via several types of non-propriety and propriety networks and protocols included mobile network and real time networks, this connectivity made the communication more reliable and convenient. At the other side, each

network and protocol has numbers of performance issues that affect the end-user processing during communication. The larger number of connectivity between several public and private networks, and deployment of protocols, caused the security issues that made communication platform venerable from several types of thread and attacks

#### IV. Research Objectives

The review has been conducted which is related with networks including traditional networks, mobile networks, real time networks and cloud computing networks performance issues and based on the review analysis following research objectives are counted as countermeasures.

- To conduct the detail review on existing performance issues lies within LAN/WAN using protocols included “transport control protocol (TCP)/Internet protocol (IP), User Datagram Protocol (UDP), OSI Protocols, Bluetooth protocols, Network time protocol (NTP), File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), Fiber Channel network protocols, Routing protocols and IEEE protocol family”. Based on detail review, the countermeasures will propose to overcome these exiting issues and enhanced the network performance, with security consideration.
- To conduct the detail review on existing performance issues lies within SCADA systems (Real Time systems via LAN/WAN) using protocols included DNP3 (Distributed Network Protocol), IEC 60870-5 Series and other, Modbus Protocol and Profibus Protocol. Based on detail

review, the countermeasures will propose to overcome these exiting issues and enhanced the network performance, with security consideration.

- This research also reviews the performance issues that are related with propriety and non-propriety protocols implementations within networks and try to find the solution to minimize the workload, while bytes transmission between propriety and non-propriety protocols or networks.
- To conduct the detail review on existing performance issues within cellular network using protocols GPRS, CDMA, GSM, WAP. Based on detail review, the countermeasures will propose to overcome these exiting issues and enhanced the network performance, with security consideration.
- To conduct the detail review, while deploying these above networks within cloud computing environment. Based on detail review, the countermeasures will propose to overcome these exiting issues and enhanced the network performance, with security consideration.
- During networks performance analysis, the existing security implementations have been also reviewed included “Firewalls, Password Protection, Secure Shell (SSH), Secure Socket Layer (SSL)/ Transport Layer Security(TLS), security patterns , cryptography security implementations and other security solutions”. Based on detail review, comparison is created between security solutions and the best generic security mechanism will propose that has potential to overcome the exiting security issues with better performance measurements.

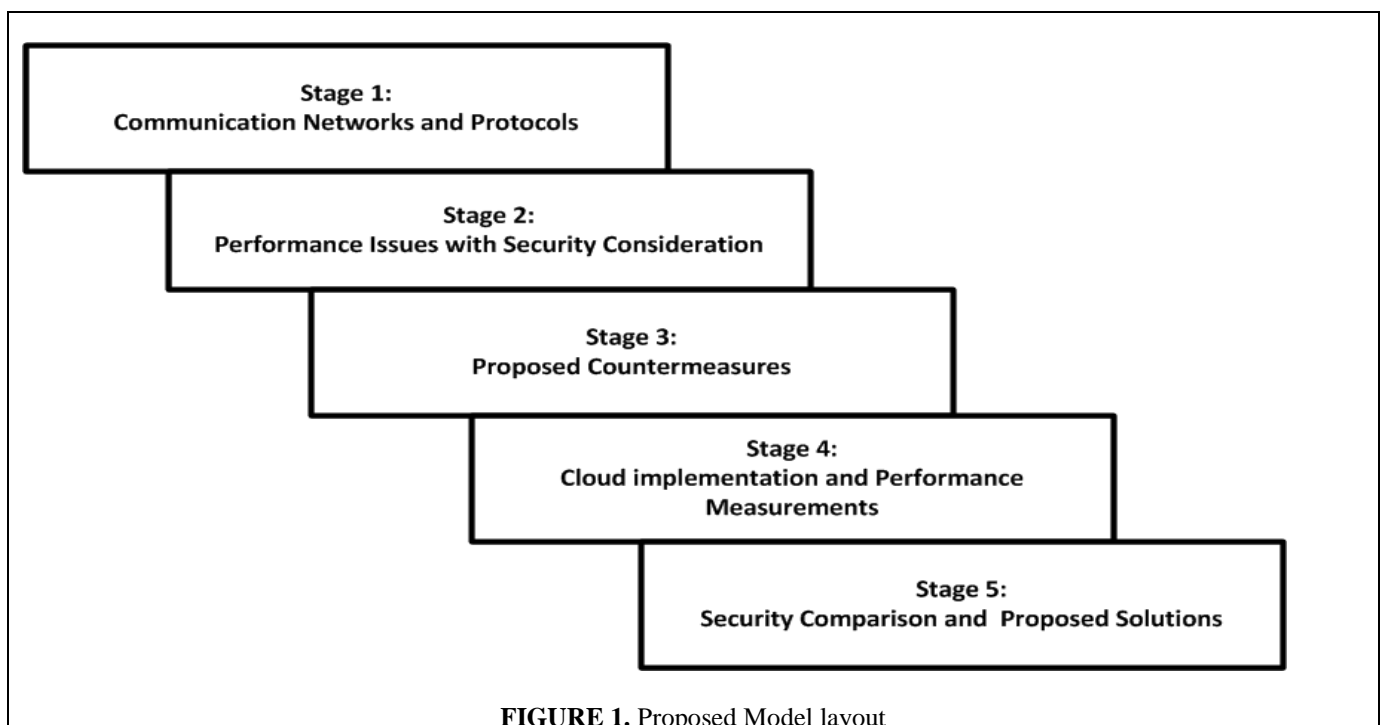


FIGURE 1. Proposed Model layout

TABLE 1. Issues and Countermeasures

No.	Issues/Vulnerabilities	Countermeasures
1.	Network miss Configuration	Need to configure the network with specified guideline/manual.
2.	No Proper Administration	Acquired proper administration policies for network management.
3.	Hardware	Compatible hardware (routers and switches, etc) is used to avoid the un-compatible issues.
4.	Status: Monitoring	Need proper check and balance system for logging nodes.
5.	Security	Need to install strong security mechanism against threads.
6.	Remote Access	Configure the remote nodes in advance, avoid others.
7.	Connections	Allow only authorized connections to access the resources and need awareness against unauthorized nodes.

## v. Modeling and Countermeasures

In figure 1, the proposed research or modeling is conducted in five stages included stage 1, stage 2, stage 3, stage 4 and stage 5. In stage 1, the detail review has been conducted that is related with the performance issues of networks such as traditional networks, mobile networks, and real time networks and protocols. In stage 2, the existing security implementations have been reviewed and countermeasures are proposed in stage 3. In stage 4, the networks implementation within cloud infrastructure has been reviewed and network performance results are measured, and security implementations are compared and new security solution is proposed at stage 5. The table 1 shows the common issues/vulnerabilities at initial stage, which are related with networks with countermeasures.

## vi. Conclusion

With the growing demands of communication infrastructures and deployment of several open networks and protocols, caused major issues in the terms of performance and security. This research thoroughly study the performance issues that are related with traditional networks, mobile networks, cloud networks and real time networks, and then proposed a generic model to overcome them. This model increases the networks performance and proper uses and placement of security mechanisms to enhance the security during communication. This research also review the importance of cloud computing infrastructure, while deploying these networks such as traditional networks, mobile networks and real time networks. This research gives new strategic ways to enhance the networks performance.

## vii. Acknowledgments

We would like to thank to our parents and our friend Mr.Irfan, boosted us morally and provided us great information resources.

## viii. References

- [1] Gregor Urbas and Tony Krone Mobile and wireless technologies: security and risk factors,2006  
<http://www.aic.gov.au/documents/E/9/9/%7bE99293FF-9E0F-4522-8E54-0598720C45B2%7dtandi329.pdf>
- [2] Landwehr, C.E. and D.M. Goldschlag, 1997, Security issues in networks with Internet access. Proceedings of the IEEE, Vol. 85, No. 12,1034-205, 1997.
- [3] S. Musa, A. Shahzad, A.Aborujilah, Simulation base implementation for placement of security services in real time environment, Proceeding ICUIMC '2013 Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, 2013,  
**DOI:** 10.1145/2448556.2448587
- [4] A. Shahzad, S. Musa, Cryptography and Authentication Placement to Provide Secure Channel for SCADA Communication, International Journal of Security (IJS), Volume (6): Issue (3): 2012,  
<http://cscjournals.org/csc/manuscript/Journals/IJS/volume6/Issue3/IJS-105.pdf>
- [5] S. Musa, A. Shahzad, 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 '2013 Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, 2013,  
**DOI:** 10.1145/2448556.2448588
- [6] S. Musa, A. Shahzad, A.Aborujilah, Mohd Nazri Ismail, Muhammad Irfan, Conceptual Model of Real Time Infrastructure Within Cloud Computing Environment, International Journal of Computer Networks (IJCN), Volume (5) : Issue (1) : 2013,  
<http://cscjournals.org/csc/manuscript/Journals/IJCN/volume5/Issue1/IJCN-269.pdf>
- [7] S. Musa, A. Shahzad, A.Aborujilah, Mohd Nazri Ismail, Muhammad Irfan, New Framework to Detect and Prevent Denial of Service Attack in Cloud Computing Environment, International Journal of Computer

- Science and Security (IJCSS), Volume (6) : Issue (4) : 2012,  
<http://cscjournals.org/csc/manuscript/Journals/IJCSS/volume6/Issue4/IJCSS-760.pdf>
- [8] Mohd Nazri Ismail, A. Aborujilah, S. Musa, A. Shahzad , Detecting flooding based DoS attack in cloud computing environment using covariance matrix approach, Proceeding ICUIMC '2013 Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, 2013, **DOI:** 10.1145/2448556.2448592
- [9] Shahzad, S., A. Aborujilah, M. Irfan , A New Cloud Based Supervisory Control and Data Acquisition Implementation To Enhance The Level Of Security Using Testbed, 2014, **DOI:** 10.3844/jcssp.2014.652.659
- [10] Shahzad, S., A. Aborujilah, M. Irfan, Secure Cryptography Testbed Implementation for SCADA Protocols Security, ACSAT 2013, IEEE, **DOI:** 10.1109/ACSAT.2013.69
- [11] 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
- [12] 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
- [13] A. Aborujilah, S. Musa, A. Shahzad, Flooding based DoS Attack Feature Selection using Remove Correlated Attributes Algorithm, ACSAT 2013, IEEE, **DOI:** 10.1109/ACSAT.2013.26
- [14] Shahzad, S., M. Irfan, Security Solution for SCADA Protocols Communication within Multicasting and Polling Scenario, Trends in Applied Sciences Research, 2014, **DOI:** 10.3923/tasr.2014.396.405
- [15] 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
- [16] Shahzad, S., M. Irfan, Key Encryption Method for SCADA Security Enhancement, Journal of Applied Sciences ,2014, **DOI:** 10.3923/jas.2014.2498.2506
- [17] Shahzad, S., M. Irfan, Deployment of New Dynamic Cryptography Buffer for SCADA Security Enhancement, Journal of Applied Sciences ,2014, **DOI:** 10.3923/jas.2014.2487.2497
- [18] Shahzad, S., A. Aborujilah, M. Irfan, The SCADA Review: System Components, Architecture, Protocols and Future Security Trends, American Journal of Applied Sciences, 2014 **DOI:** 10.3844/ajassp.2014.1418.1424
- [19] Shahzad, S., A. Aborujilah, M. Irfan, The Security Survey and Analysis on SCADA Communication, Journal of Computer Science, 2014, **DOI:** 10.3844/jcssp.2014.2006.2019
- [20] Roger M. Needham and Michael D. Schroeder. 1978. Using encryption for authentication in large networks of computers. *Commun. ACM* 21, 12 (December 1978), 993-999. **DOI:** 10.1145/359657.359659
- [21] Ning Wang; Ning Zhang; Gulliver, T.A., "Cooperative Key Agreement for Wireless Networking: Key Rates and Practical Protocol Design," *Information Forensics and Security, IEEE Transactions on* , vol.9, no.2, pp.272,284, Feb. 2014. **DOI:** 10.1109/TIFS.2013.2293113
- [22] Oliveira, P.F.; Barros, J., "A Network Coding Approach to Secret Key Distribution," *Information Forensics and Security, IEEE Transactions on* , vol.3, no.3, pp.414,423, Sept. 2008. **DOI:** 10.1109/TIFS.2008.928538
- [23] Nabil, S.; Mohamed, B., "Security solution for semantic SCADA optimized by ECC mixed coordinates," *Information Technology and e-Services (ICITeS), 2012 International Conference on* , vol., no., pp.1,6, 24-26 March 2012. **DOI:** 10.1109/ICITeS.2012.6216629
- [24] Zhu, Y.; Ahn, G.-J.; Hu, H.; Ma, D.; Wang, S., "Role-Based Cryptosystem: A New Cryptographic RBAC System Based on Role-Key Hierarchy," *Information Forensics and Security, IEEE Transactions on* , vol.8, no.12, pp.2138,2153, Dec. 2013. **DOI:** 10.1109/TIFS.2013.2287858