Cryptography and Authentication Placement to Provide Secure Channel for SCADA Communication

AAmir Shahzad mail2aamirshahzad@gmail.com
Malaysian Institute of Information Technology (MIIT)
University Kuala Lumpur,Malaysia

Shahrulniza Musa shahrulniza@miit.unikl.edu.my
Malaysian Institute of Information Technology (MIIT)
University Kuala Lumpur,Malaysia

Abstract

Distributed control systems (DCSs) and Supervisory Control and Data Acquisition (SCADA) systems are widely used in real time industry infrastructures such as water pumping stations, gas, and oil and other real time deployments. SCADA implementation within a cloud computing environment is new and beneficial for real time infrastructures. Using cloud computing, real time infrastructure saves cost, achieves more reliability and functionality related to the current requirements of industry in the term of control and acquisition. In current paper, the cryptyography algorithms are implements to secure data, and a conception model is proposed to implement SCADA within cloud environment and also discuss the security issues related to SCADA, and cloud computing. At the end; cryptographic solution is implemented in SCADA communication without or/and within the cloud infrastructure (Delivery of data/message from the Master terminal unit or MTU to Remote terminal unit or RTU) to achieve security services.

Keywords: Supervisory Control and Data Acquisition (SCADA), Cloud Computing,Cryptography, SCADA and Clould Computing Security Issues.

1. INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) systems are distributed geographically all over the world and control from a centralized location. SCADA Systems is wildly deploying over real time infrastructure sectors such as water distribution and wastewater collection systems, oil and gas pipelines, electrical utility and distribution, rail and public transportation systems. SCADA systems collect the information that is distributed among different locations and process to the main station, and monitor and control SCADA network devices during incoming/outgoing transmission. Scada systems are a combination of hardware and software. More detail is depicted in the next section. Distributed control systems are used in industry for controlling production within the same geographical location. Pharmaceutical processing, water distribution and wastewater collection systems, oil and gas pipelines, electrical utility and distribution, rail and public transportation systems are examples of DCSs deployment [1].

Cloud computing is new and advance technology in information technology infrastructures that uses remote server and internet to process and maintain data, and other software/hardware applications within cloud networks. Using Cloud computing users can access any application and resources within a cloud infrastructure without any installation [2]. More detail is depicted in the next section.

SCADA system within cloud computing is relatively new technology that provides convenient, on-demand network access to resources such as networks , servers, storage, applications , and

services. Using SCADA system within cloud computing, user significantly saves cost, more reliability and achieves more functionalities related to their needs , and requirements and also allow users to access SCADA or view SCADA device status information using smart phones such as iPhone, Android and others , laptops and tablets PC [3].

2. ARCHITECTURE

‘‘SCADA (Supervisory Control and Data Acquisition)’’ systems are uses for industrial equipments controlling and monitoring purposes.SCADA uses three generations for defining the architecture such as ‘‘First Generation: Monolithic SCADA, Second Generation: Distributed SCADA, Third Generation: Networked SCADA’’[4].

In the first generation of SCADA system; SCADA system was operated as standalone system without connectivity with other systems (networks). Wide area network (WAN) was not used (implemented) by SCADA system at all, but the WAN concept was used to connect remote terminal station with master station or SCADA server. In the second generation of SCADA system; LAN technology was used and several stations were sharing the information between them. The stations were connected within LAN network and perform specific operation and shared the information with other stations (real time information). These stations in LAN network were mini computers and every station perform specific operation (function).Several LAN networks were designed and communication with each other (WAN) but still limited to make connection with other network.In the third generation of SCADA system; open standard protocols are uses rather than proprietary protocols. Several stations have been connected with SCADA networks and sharing information (real time information) uses of WAN technology rather than only LAN with open standard protocols. Current generation also uses ‘‘off-the-shelf systems’’, to connect the stations (users) with the devices (peripheral) available within network. The most important advantage in current generation, is the uses of WAN protocol (Internet Protocol) and provide communication ways between master station and remote station (remote device) and/or remote station (remote device) and master station [4].

SCADA usually have five main component/parts such as master station, remote station, and HMI, historian and communication network. Master station is supervisor in communication network and uses to control and send request to remote station, and remote station collect the information from LEDs and sensors and send response to master station.‘‘HMI (human machine interface)’’ is graphical software uses for user interaction between master station and remote station and etc. Historian is uses for data/information storages purposes and exit within master /remote station (shared) and/or separate station (computer) [4]. User can view and access information from historian via ‘‘human machine Interface (HMI)’’.

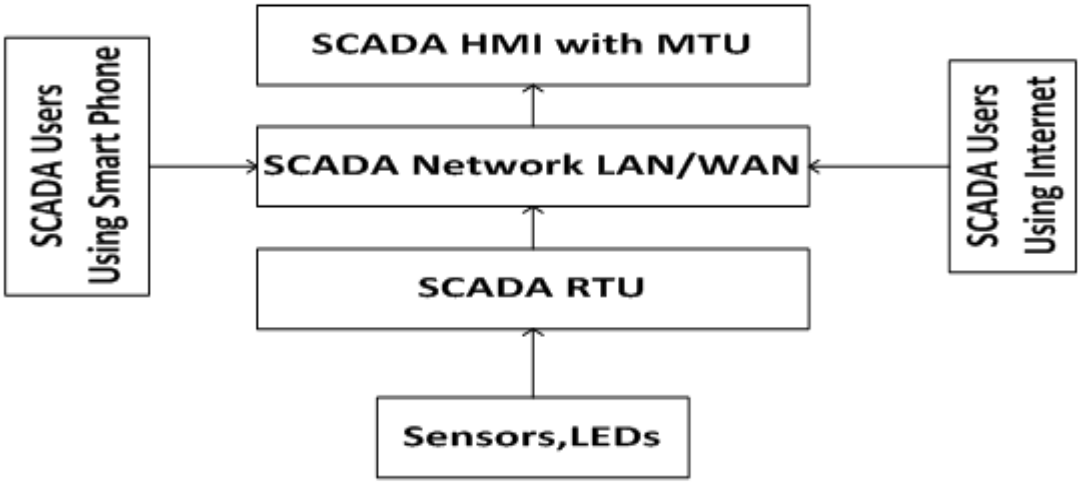

FIGURE 1: SCADA Architecture

SCADA system uses networks like LAN/WAN for communication between several devices within a defined SCADA network. SCADA uses several types of topologies such as bus, star, and mesh (In the case end to end) but limited within SCADA protocols such as DNP3, Modbus and Field bus etc. These protocols have their own functional requirements and specifications for data/message construction and processing.

Open system Interconnection model was define by international standard organization (ISO), use for data communication system and data communication flow is in hierarchical manner, from bottom to top, the bottom layer start from physical layer and move to application layer.Below figure shows the architecture of ISO model.

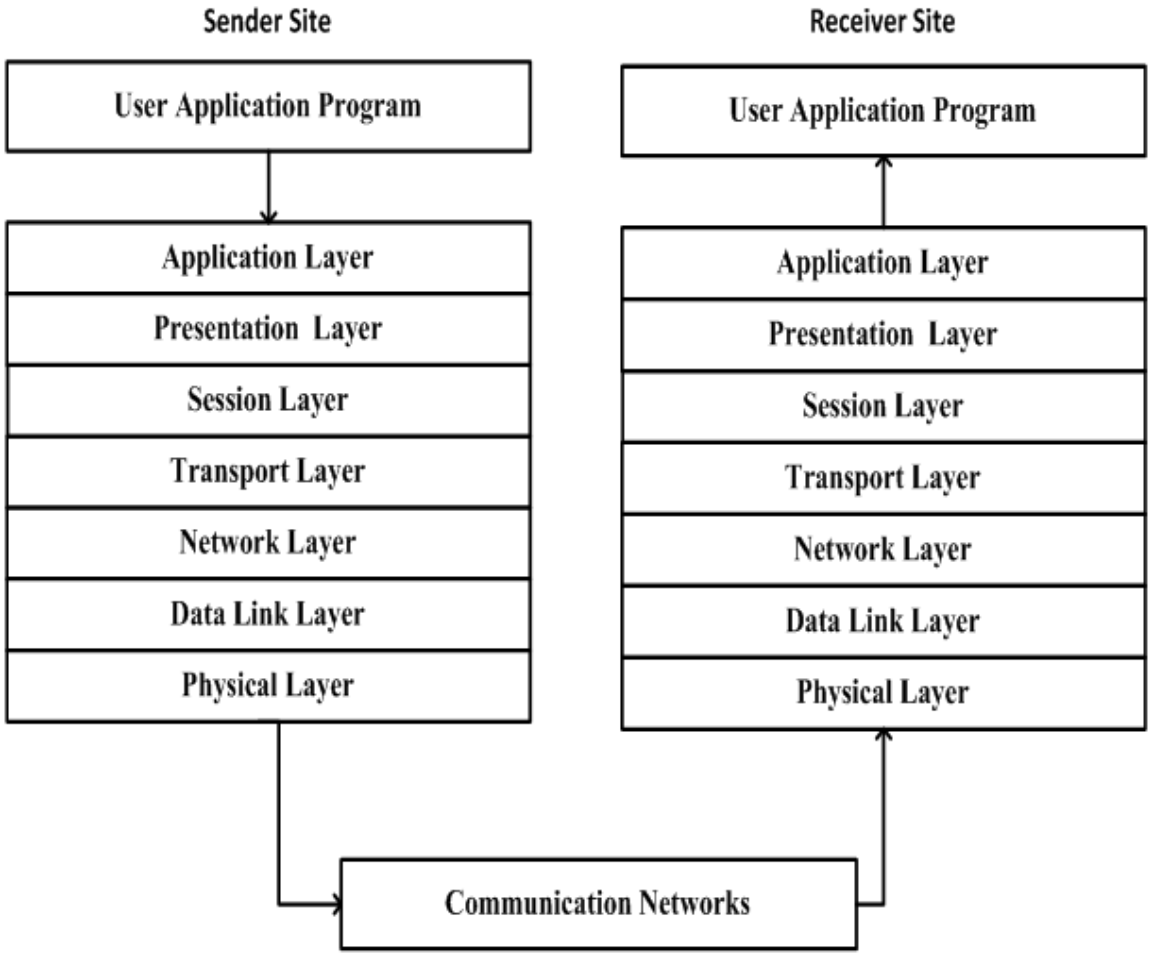

FIGURE 2: ISO Architecture

Distributed network protocol (DNP3) is one of the famous protocol uses in SCADA systems. The International Electro Technical Commission (IEC) defined a three-layer model (Such as the application layer, transport layer and physical layer) called enhanced Performance architecture (EPA) model and DNP3 is based on this model. Below figures depicts the architecture of the SCADA DNP3 protocol and relationship between OSI model and EPA model.

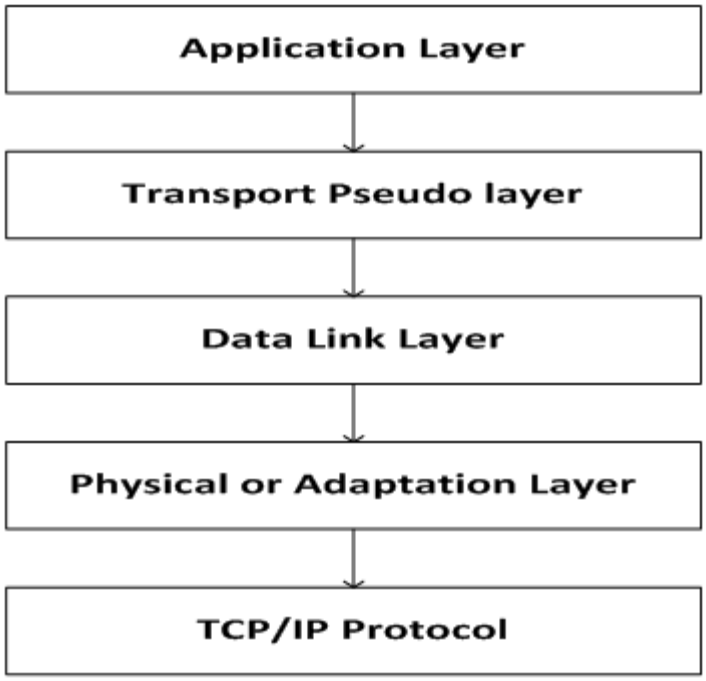

FIGURE 3: SCADA DNP3 Architecture

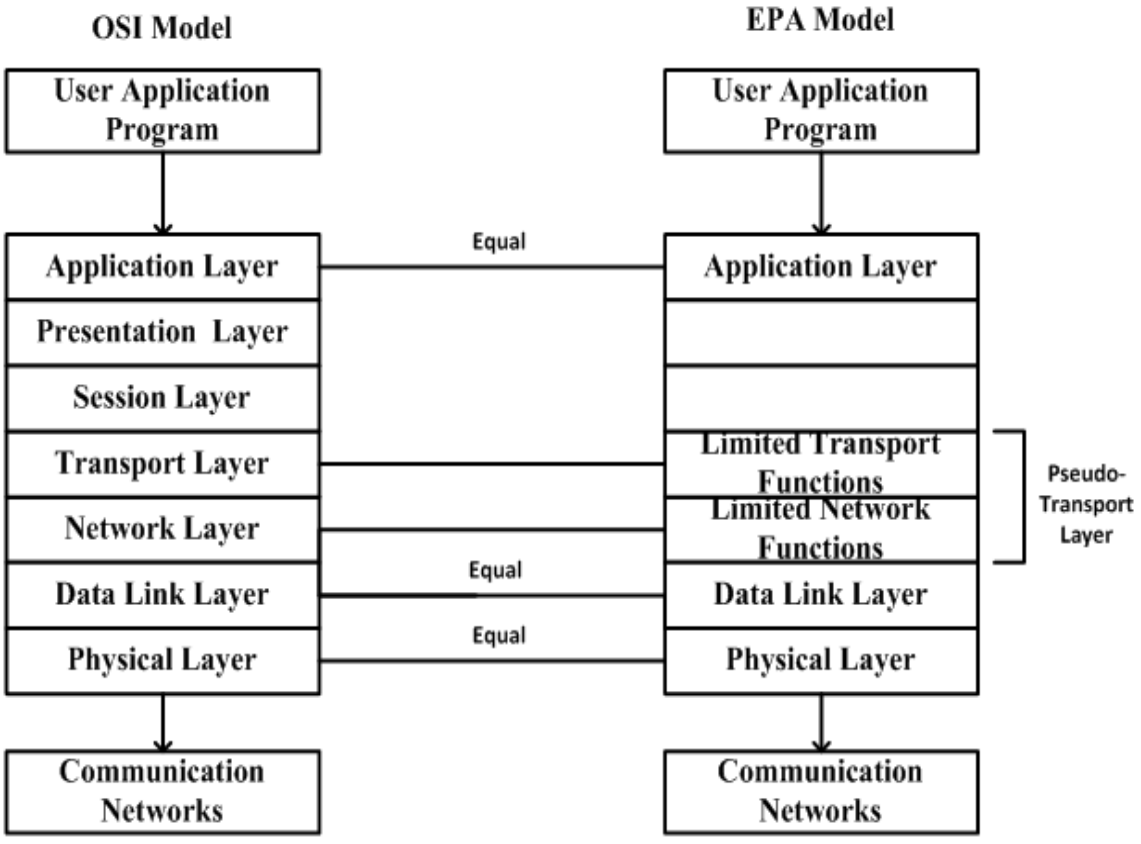

FIGURE 4: Relationship between ISO model and EPA model

Modbus is a serial application layer message (such as request, confirmation, indication and response) protocol base of OSI seven layer model and provides communication between the devices connect with SCADA network. Below figure depicts the architecture of SCADA Modbus protocol.

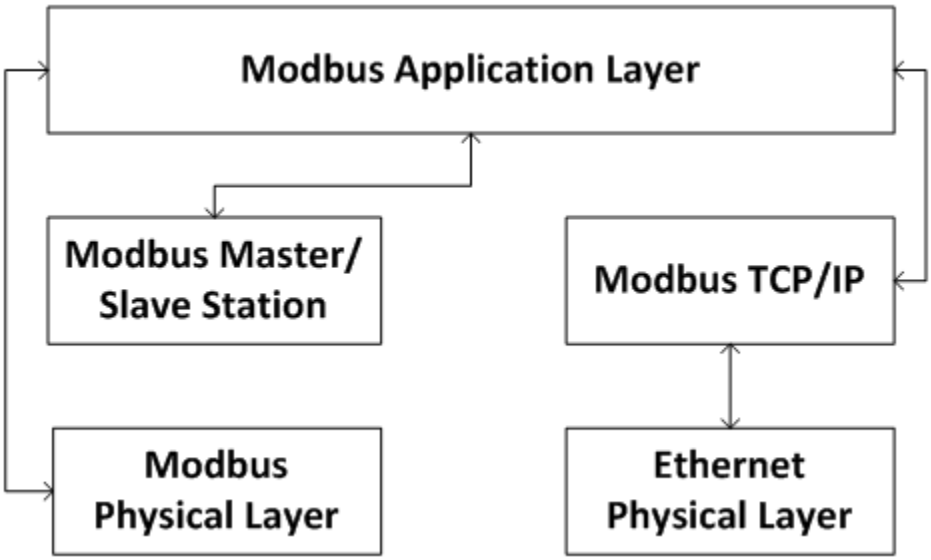

FIGURE 5: SCADA Modbus Architecture

Fieldbus is another industrial protocol that provides reliable distributed communication control to the connect SCADA devices and mostly based on serial communication. Below figure depicts the architecture of the SCADA Fieldbus protocol.

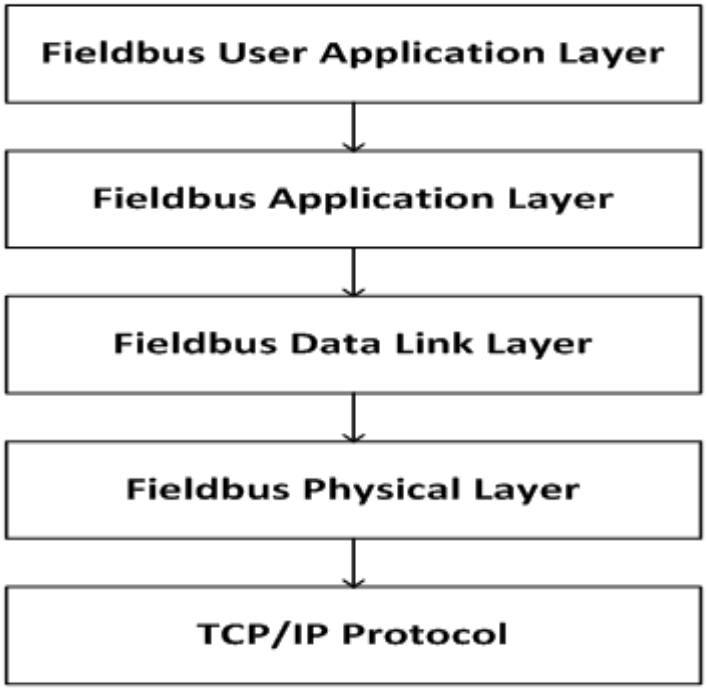

FIGURE 6: SCADA Fieldbus Architecture

Profibus is international networking standard,uses for process control and in large assembly and material handling machines.Single-cable wiring of multi-input sensor blocks, pneumatic valves,complex intelligent devices, smaller sub-networks , and operator interfaces are supported by Profibus. Below figure depicts the architecture of the SCADA Profibus protocol stack.

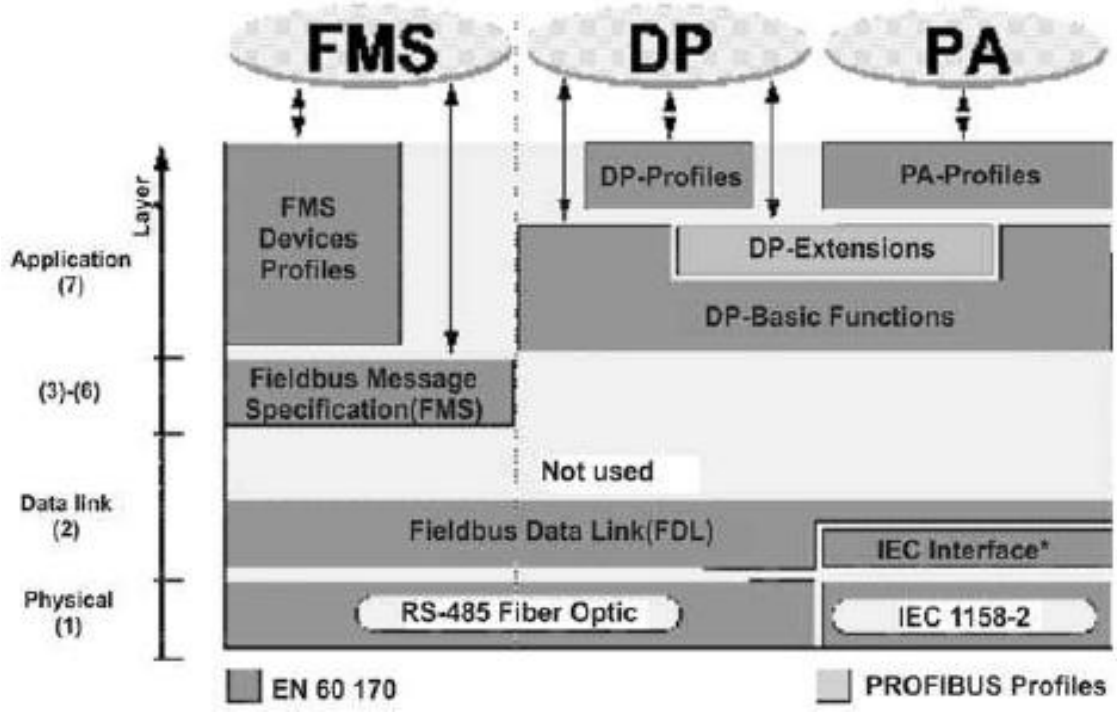

FIGURE 7: SCADA Profibus Protocol Stack
(Ref: Figure 14a.1, http://www.scribd.com/doc/53430270/80/Understanding-the-DNP3-message-structure)

Cloud computing has three basic categories such as public cloud, private cloud and hybrid cloud, and three fundamental models such as Infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

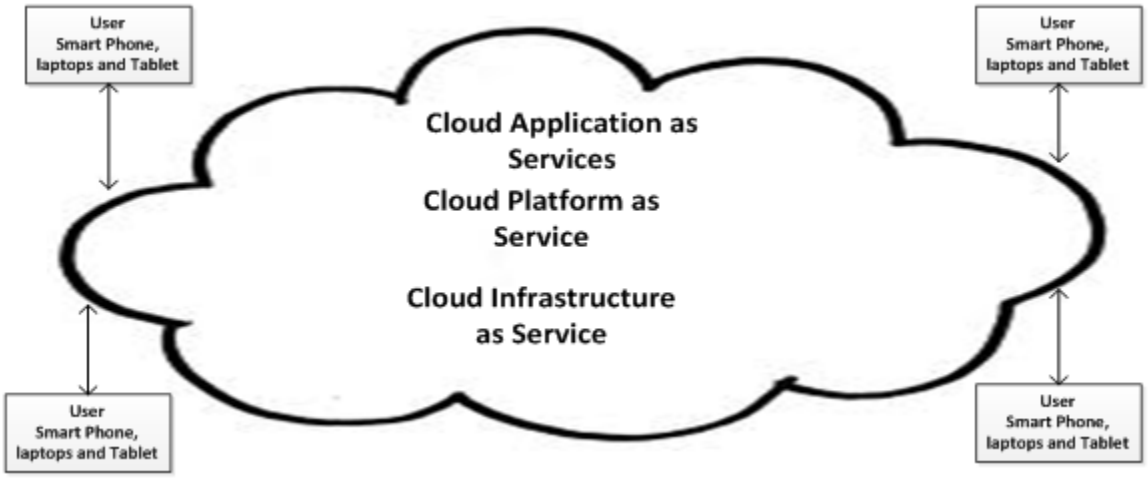

FIGURE 8: Simple Cloud Computing Architecture

Public cloud services and applications are free to access or download by any user (public) such as Google, Amazon and Microsoft etc. are the examples of public clouds. There are also many types of public cloud such as Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Storage as a service (STaaS), Security as a service (SECaaS), Data as a service (DaaS), Database as a service (DBaaS), Test environment as a service (TEaaS), Desktop Virtualization, API as a service (APIaaS) and Backend as a service (BaaS). Private cloud is base on single organization, the infrastructure that is used by one company and handle by own or may by authorized third party. Hybird cloud is base on the public and priThat cloud infrastructure and last, community cloud base of shared infrastructure between companies and/or organizations for specific work such as in the term of security matters [5].

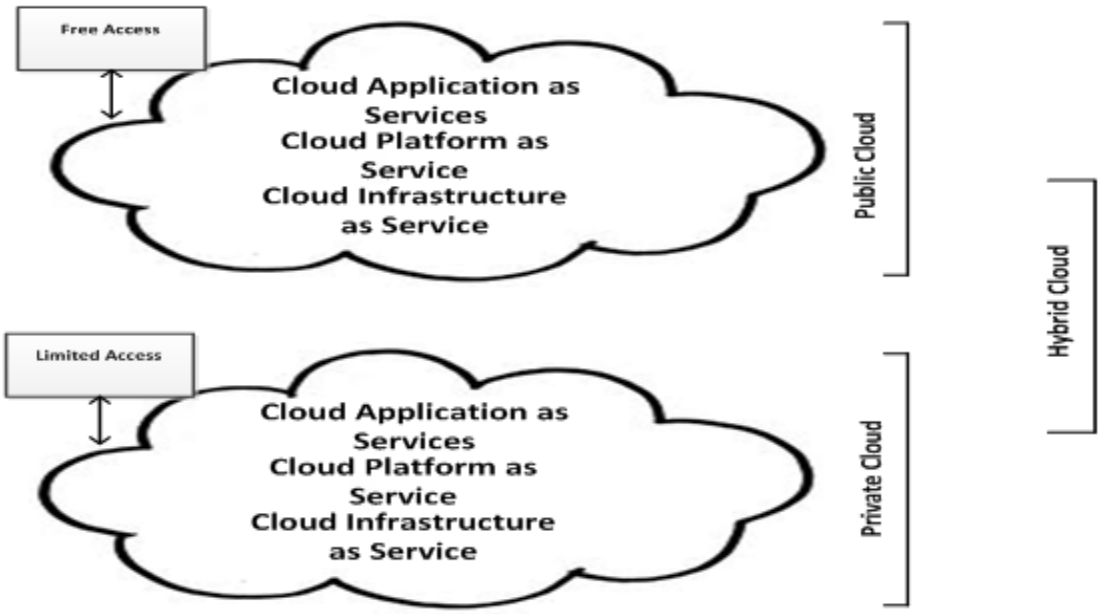

FIGURE 9: Public, Private and Hybrid Clouds

Infrastructure as a service (IaaS) is the basic infrastructure of cloud computing that provides hardware as computers or virtual machines and resources such as virtual machine image library, resource pooling from data center, virtual local area networks (VLANs), IP addresses, data and file storage, load balancers, firewalls and etc. The second Infrastructure, platform as a service (PaaS) provides platforms such as web server, operating system, programming language (such as Java, C/C++, C#) execution environment, databases (such as mysql and oracle) etc. . Software as a service (SaaS) provides software applications installation and operation (Google applications, Microsoft office are examples of Software as a service), users can access the applications from could base on the requirements [5].

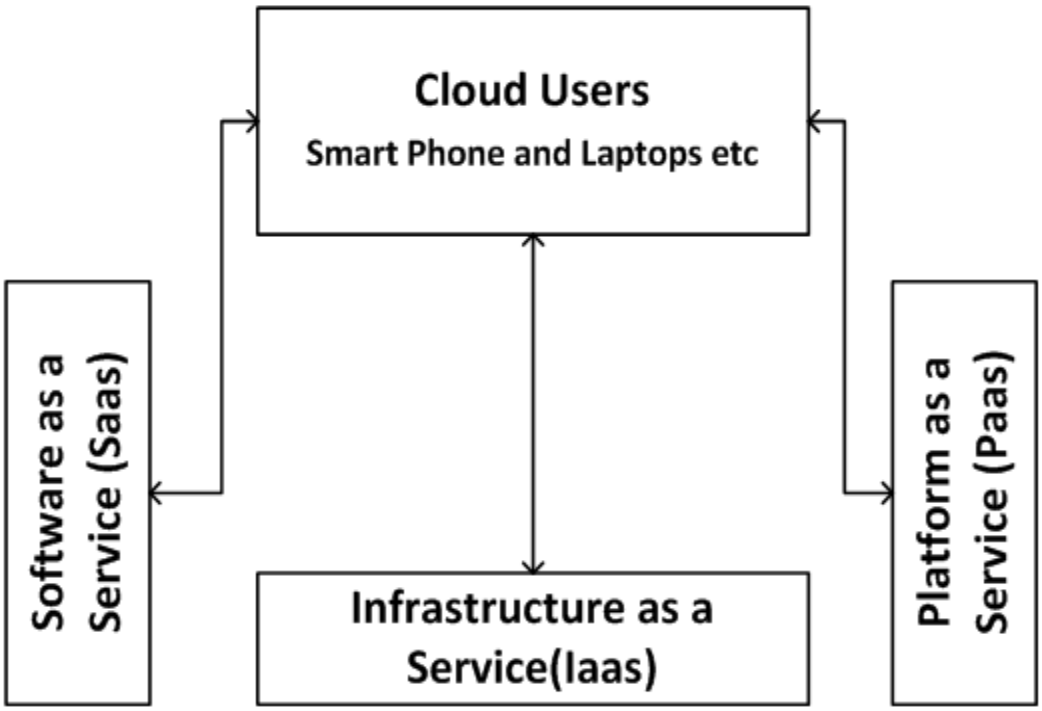

FIGURE 10: Cloud Services Infrastructure

3. LITERATURE REVIEW

In [6] , explain in detail the SCADA system , and attacks related to SCADA and systematically approach is used for identifying and classifying attacks on SCADA and major challenges related to SCADA security (cyber security).

In [7], paper study and explain insecure/insecurity part of SCADA protocol design especially SCADA Modbus protocol using exploitation and monitoring. Make detail analysis when an insecure message / frame is sent from the master to the outstation. So, by using this, users can identify the security flaw and find the ways to fix the security flaws. Also give mechanism to protect SCADA communication.

In [8], detail explanation about several types of cryptography attacks such as Side Channel attacks, Brute Force attacks, Meet-in-the-Middle attack. In [9], paper implements an intrusion prevention system for SCADA without changing in the functional part of the SCADA system. Explain the attack vector related with SCADA threads and solutions to protect SCADA from attacks.

In [10], explain various types of attacks on networks and how to defense team.In [11], propose guidance to secure real time infrastructure/industry control infrastructure such as supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other systems. In [12], explain the effect of DDOS and how to detect it in the application layer and propose a Pearson correlation coefficient method to detect the application-layer-based DDoS attacks.

In [13], explain and classify the DDoS and QoS attacks approaches, and propose network monitoring techniques for service violations. At the end of the paper , comparison is created

between schemes used and identifies which one is the best scheme as compared with other schemes.

In [14],"Safe and Secure Integration of Automation Systems and Enterprise IT Infrastructure Using Cloud", they suggest cloud and SCADA integration architecture after he gave briefly summary about IT enterprise and SCADA architecture in Separate way. Then the paper gives shortages of the separate SCADA system and IT infrastructure such as needing to outsource IT maintenance staff and another team to the SCADA system , increasing cost . Secondly advantage of using SCADA with cloud is listed such as IT issues overhead can be reduced by using the cloud. Securing IT and SCADA system using same policy can be more cost effective as well as management , after that , simple high level modeling is given and the paper give more attention to some problem can be existed such as security and safety problems. Finally, some of the benefits and shortages moving SCADA applications to the cloud have been listed. Benefits such as on demand resources, and cost reducing and more flexibility. In another side some of disadvantage can be observed especially security side.

In [15] a new model has been suggested which integrate the cloud with SCADA system called VS-Cloud. This new system can enhance SCADA efficiency and reliability. However, security shortages are still the main problem. In this article, some of security mechanism has been proposed especially in data cryptographic side, which can assist in SCADA and cloud integration process.

In [16], the paper suggested to utilize a high computational power in cloud in grid network which need the high computational capacity and real-time monitoring. In addition, they implement some laboratory experiment to load forecasting application in the power management domain. This experiment has been done to measure the processing power and performance of cloud computing in the renewable power application field.

In [17], SaaS (Software as a Service) cloud model is suggested to install SCADA applications in the cloud instead of installing SCADA on local computers. Moreover Benefits of moving the SCADA system into the cloud are also listed which Includes reduced cost because in cloud the cost policy according to the usage. In another side SCADA hardware and application can be up to date constantly and therefore no need for more effort in hardware and software maintenance.

In [18], some of the benefits and shortages moving SCADA applications to the cloud have been listed. Benefits such as on demand resources, and cost reducing and more flexibility. In another side some of disadvantage can be observed especially security side.

In [19], provides detail related to SCADA system security protection and suggest a solution to secure SCADA communication. Part 1 gives detail about SCADA cyber security goals and their fundaments, and then defines cryptography requirements, constraints and test plan acquired two American Gas Association 12 series. In [20], Wrap SCADA protocols discuss two ways, IPSec protocol and Secure Sockets Layer (SSL) /Transport Layer Security (TLS) protocol was implemented to secure client/server application against from attacker that try to delete, replay and modifying message/data in network transmission. Enhances SCADA protocols with selected Cryptography techniques compare the security mechanism between SSL/TLS and IPSec with Cryptography. SSL/TLS and IPSec provide security in selective part of communication but using cryptography solution provides end to end security in communication. Authentication Octets check the data integrity in SCADA communication by sending addition bytes of data appended to each message when communication starts from client to server or server to client.

In [21], paper proposes several techniques for public key distribution and uses Diffie-Hellman algorithm for key exchanges between sender/receiver and gives details about the man-in-the

middle attack counter measures.In [22],authors review the the constraints and requirements for SCADA ,and related security and than propose a suitable architecture for secure SCADA communications.Paper also generally explain the architecture of SCADA System and security requirements of SCADA such integrity,confidentiality and availability and make review on best way to protect SCADA from malicious attacks.

In [23], Paper explain general concept of SCADA system and their connectivity between other networks and security related with SCADA system. Discuss the web security and SCADA connectivity with web and then propose the symmetric key encryption for SCADA web security. Supervisory Control and Data Acquisition (SCADA) systems are distributed geographically all over the world and control from a centralized location. SCADA systems collect the information that is distributed among different locations and process to the main station, and monitor and control SCADA network devices during transmission. SCADA systems were traditional used the ‘‘PSN (Public Switched Network)’’ for network communication, devices (field devices) monitoring and controlling purposes [4].

In [24], paper start with widely investigation of exiting proposed mechanism related with SCADA Security and highlight also international standard organizations standard for securing SCADA systems. Paper overview SCADA architecture and constraints such as Resource constrained RTU high resiliency, low bandwidth and low latency communication, long node life, real time Structured network, phased Delivery, RTUs physically insecure, RTU clocks initially unsynchronized, RTU clocks synchronized after initialization then, explain challenges such as Key management, peer-to-peer communication mode , broadcast communication mode , Intrusion detection , Transition , for the SCADA security such as spoofing, modification, replay ,eavesdropping on key exchange only and summarize the current results from exiting works done by researchers in terms of SCADA security.

In [25], paper explains SCADA system architecture its monitoring and controlling parts and SCADA data communication ways and time related with data communication. Explain SCADA security issues and IP-based standards, and the probability and impact of cyber attacks on SCADA system. Papers review the threads and vulnerabilities related with SCADA system and propose general idea base on symmetric and asymmetric algorithms to secure SCADA communication. In [26], paper start with general concept related with SCADA and advantages such as in the terms of control, data viewing and generation. Explain terms related with web SCADA and security issues such as lack of security and authentication in the design, deployment and operation of existing SCADA networks, SCADA systems protocols and proprietary interfaces, SCADA physically security, SCADA Internet disconnected, IP Performance overhead with Internet connectivity and propose crossed-crypto-scheme for web SCADA security as a countermeasure

In [27], article explain architecture of SCADA system and examines specific existing SCADA systems aspects that are vulnerable to cyber attack and define cryptographic mechanisms to addresses SCADA security and mitigate risks.In [28], Paper discuss general terms related with SCADA and distributed network protocol (DNP3).Thoroughly discuss the architecture of distributed network protocol (DNP3) and propose a conceptual mechanism to secure DNP3 protocol as data link layer. Paper define new structure as DNPSec with five fields such as new header, key sequence number, original LH header, payload data, and authentication data. In original LH header field, 4 bytes are multiply of 264 bytes and provides boundaries of 64 bits to support the encryption algorithms. Which support the encryption algorithms such as Data encryption standard (DES).

In[29], Paper describes Supervisory control and data acquisition (SCADA) system structure and lack of security in SCADA system and attacks related with them. Paper proposes vulnerability and threat analyses as methods for testing new SCADA security models. Use two security

models for enhancing SCADA communication protocol such as Authentication via Digital Signatures and Authentication via Challenge Response for enhancing SCADA communication protocol.Also specify the attacks such as Modification attack, Spoofing, Man-in-the-middle attack, Non-repudiation, Replay attack, Eavesdropping. In [30],research identifies SCADA threats and investigates methods to enhance DNP3 protocols security and explain methods such as SSL/TLS, IPsec, object security, encryption, and message authentication object for securing SCADA systems.

In[31], discusses internet SCADA, its connectivity with internet through a wireless network and also security consideration related to wireless SCADA. Base on these security issues Rosslin John Robles and Min-Kyu Choi proposes a solution to overcome security issues related to SCADA communication, and propose RC4 cipher algorithm to secur SCADA internet security and internet security issues such as lack of security and authentication in the design, deployment and operation of existing SCADA networks, SCADA systems protocols and proprietary interfaces, SCADA physically security, SCADA Internet disconnected, IP Performance overhead with Internet connectivity.

In [32], Paper propose general idea to use Advance encryption standard (AES), RSA,MD5 and Elliptic Curve Cryptography to achieves integrity, confidentiality and authentication of data.In [33], using Symmetric cipher (AES-Rijndael) and public key cryptography (RSA) with hash function SHA-512 to secure data during communication and address security primitives such as integrity, confidentiality and authentication.

In [34], Cryptography algorithms such AES and RC4 are uses within wireless Local area network(WLAN). Small packets are used by AES algorithm and large packets are used by RC4 algorithm according to analysis of research results. In [35], Paper uses AES algorithm with blocks size 128, 192 or 256 bits and key lengths of 128, 196 and 256 bits and RSA algorithm to secure data.

4. PROPOSED WORK

In proposing cryptography solution, MTU generate a new secret key using AES algorithm (In DNP3 protocol, application layer take data/message from the user application program) and encrypt the message (data/message has taken from the user application program) using the same key. MTU message (requested) also subjected to a SHA-1 algorithm for integrity value check. So, MTU message used the input to SHA-1 hashing algorithm to generate a hash value it's also represented the message digest, and then encrypted message digest by Private Key using RSA algorithm. This produced function as a digital signature to verify the non-repudiation security service.

Where, encrypted message + encrypted message digest (SHA-1) = Message 1

The above all encryption and hash function process is repeated one more time but in hash case, SHA-2 is used. So, MTU generate a new secret key using AES algorithm and encrypt the message 1 (data/message has taken from the first encryption process)) using the same key. MTU message1 also subjected to a SHA-2 algorithm for integrity value check. So, message1 used the input to SHA-2 hashing algorithm to generate a hash value it's also represented the message1 digest, and then encrypted message1 digest by Private Key using RSA algorithm. This produced function as a digital signature to verify the non-repudiation security service. Then MTU send Message2 to RTU.

Where, encrypted message1 + encrypted message1 digest (SHA-2) = Message 2

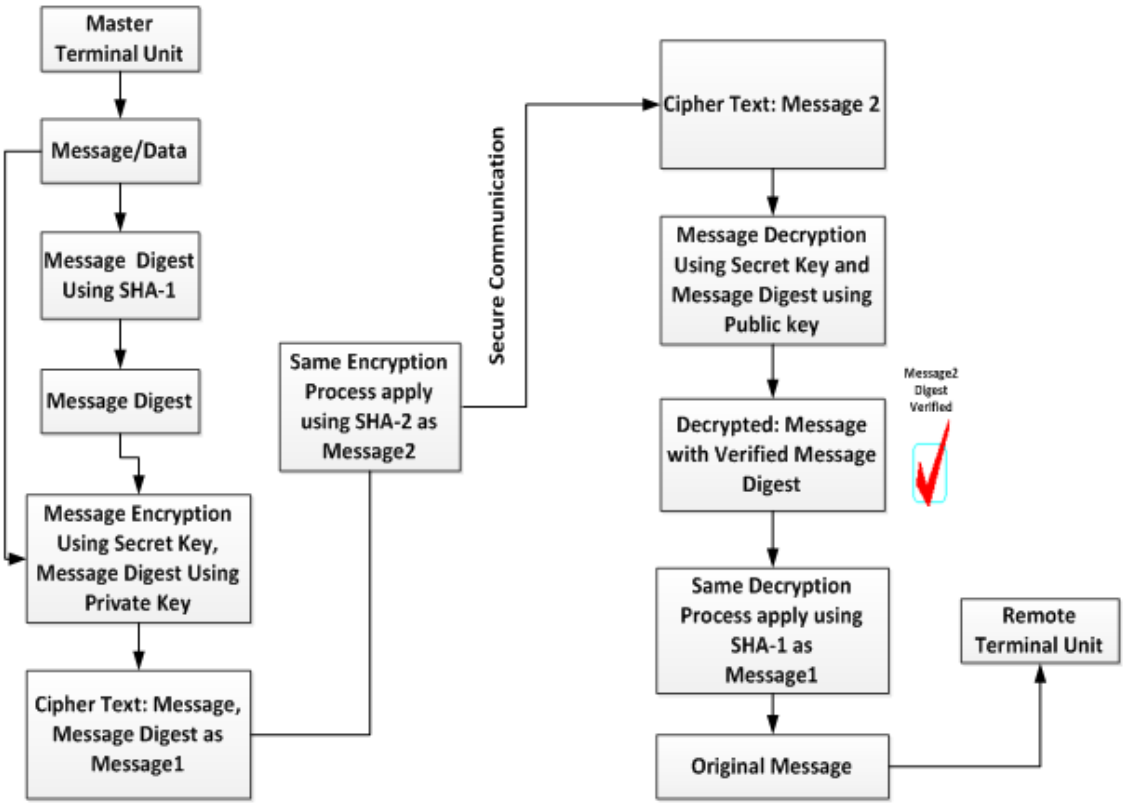

FIGURE 11: Propose Cryptography Solution

On the receiving side, RTU uses his private Key to decrypt the Message2. When Message 2 will decrypt successes, mean that we get decrypted secret key and also with a message1 digest. Then RTU uses the secret key to decrypt the message1 and decrypted message again subjected to SHA-2 hash algorithm to compare with decrypted message1 digest to ensure integrity of data. Here, Message 1 (encrypted message and encrypted message digest) is again subjected to the decryption process because at the MTU side encryption process was implemented twice. So, RTU uses his private Key to decrypt the Message1. When Message1 will decrypt successfully, mean that we get decrypted secret key and also with a message digest. Then RTU uses the secret key to decrypt the message and decrypted message again subjected to SHA-1 hash algorithm to compare with decrypted message1 digest to ensure integrity of data. Now finally we get original message. This is not possible for an attacker to attack on message because the message is encrypted twice or if the attacker encrypted successfully but the original message is still saved. We can conclude that propose a solution, verify the security services such as authentication, integrity, non-repudiation and confidentiality of data in SCADA systems. For more detail related to the attacks, and propose solutions are illustrated in the table below and our testbed (Figure 8) is based on three Remote terminal units (RTUs) connected with one Master terminal unit (MTU) using the TCP / IP protocol.

Attack Type	Attack Detail	Cryptography Solution
Integrity Attacks	Frame and Data/Message Deletion	SHA-1 and SHA-2
Authentication Attacks	Guessing Shared Key, Brute force	AES and RSA algorithms
Confidentiality Attacks	Eavesdropping, Key Cracking, Man in the Middle	AES and RSA algorithms
Non-Repudiation	Original MTU/RTU or Sender/Receiver	Digital Signature (Using Hashing and RSA algorithms)

TABLE 1: Major Attacks

Methods	Advantages	Disadvantages
IPSEC (Internet Protocol Sec)	Provide Integrity and Authentication	Depending on Cryptography algorithms
SSL (Secure Socket Layer)	Provide Integrity and Authentication	Depending on Cryptography algorithms
TLS (Transport Layer Security)	Provide Integrity and Authentication	Depending on Cryptography algorithms
Cryptography	Provide Integrity, Confidentiality, Non-Repudiation and Authentication	Depending on Complex Mathematic functions

TABLE 2: Security Anaylsis

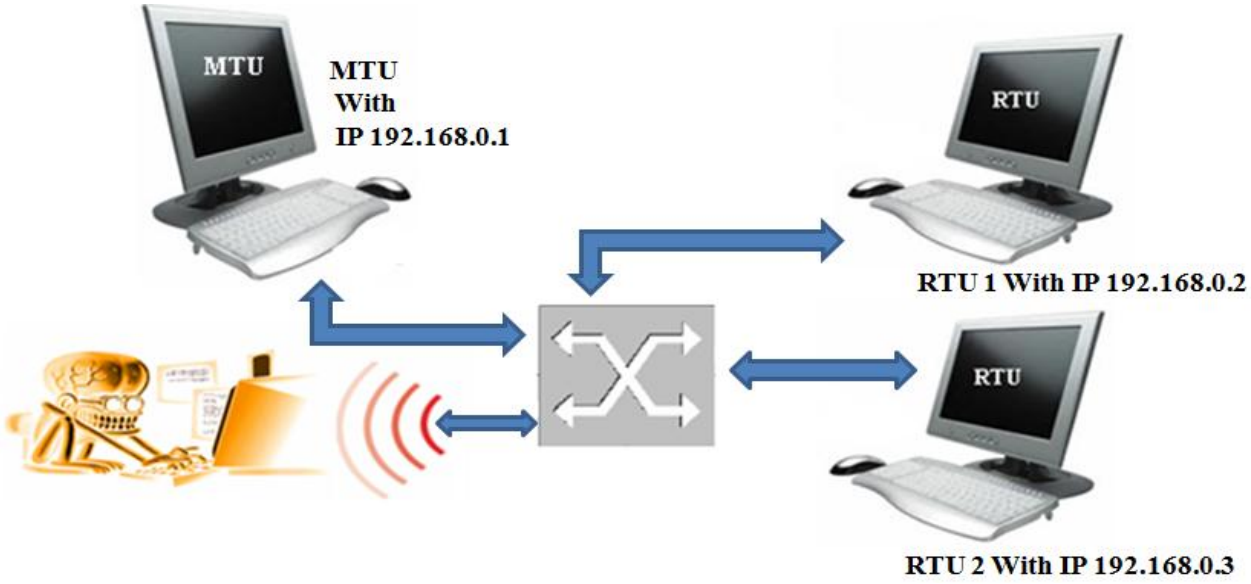

FIGURE 12: Connectivity between the MTU and RTUs

We have proposed two scenarios; bases on hybrid cloud infrastructure, to put SCADA application within cloud infrastructure. In the first scenario; SCADA applications are processed entirely inside the cloud and simultaneously all executions will save in Master Station.

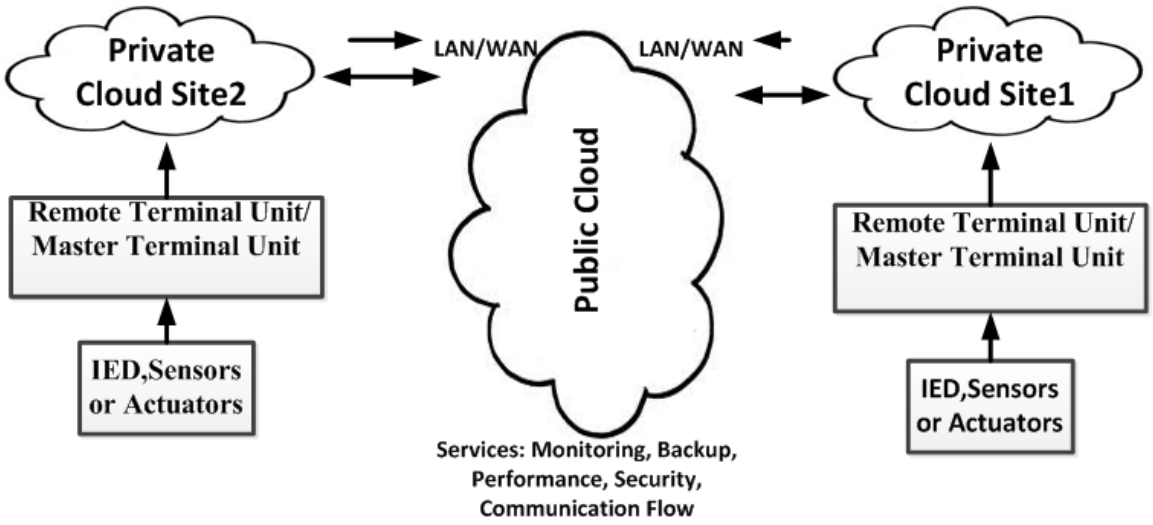

FIGURE 13: SCADA Cloud Scenario 1

In a second scenario; SCADA applications are running in separate application server directly connected to devices in SCADA network, and send information to cloud for monitoring and storage and simultaneously all executions will save in master station.

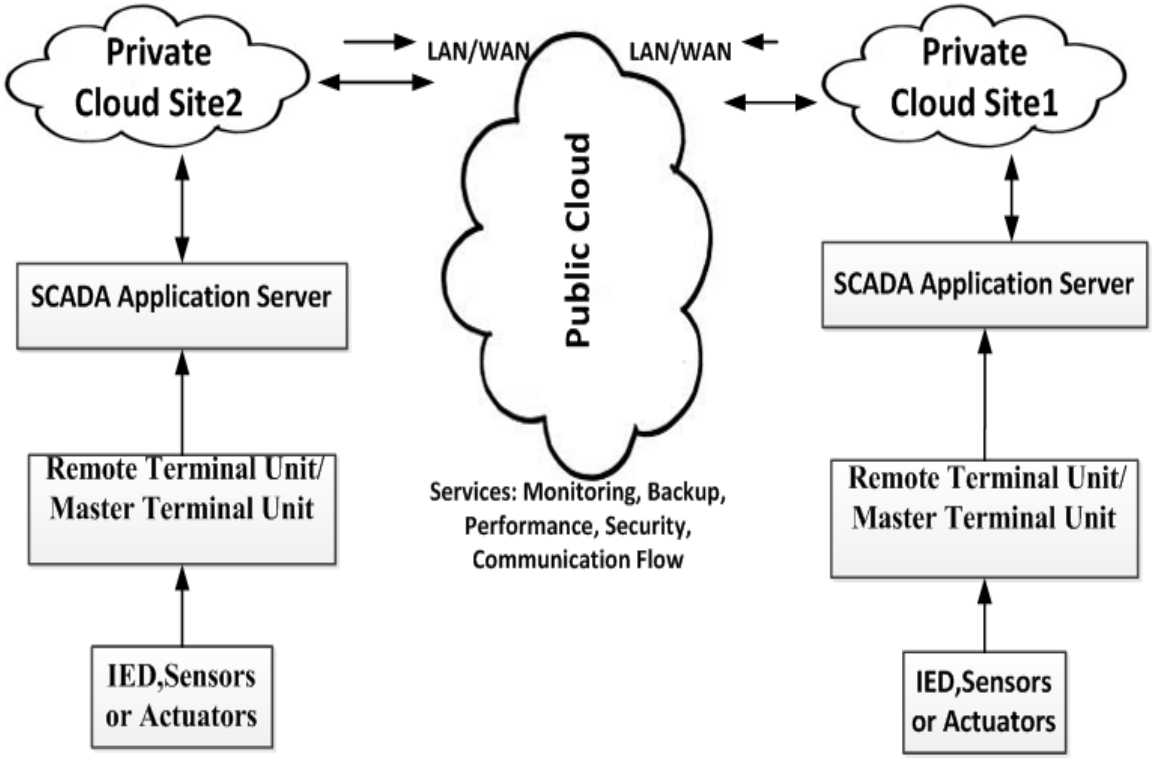

FIGURE 14: SCADA Cloud Scenario 2

Each time before data/message is sent or receive input to cryptography solution, apply the encryption process define above and then send or receive by MTU/RTU. Encryption/decryption process verify the security services (such as authentication, integrity, non-repudiation and confidentiality) on data/message requested from MTU to RTU or/and RTU to MTU. We conclude that the data / message is secure during transmission.

5. CONCLUSION and FUTURE WORK

Current paper, discuss the security related with real time system such as SCADA and DCS, and give solutions to secure these systems using cryptography algorithms. Using solution as a hybrid form (algorithms: RSA, AES, SHA-1 and SHA-2) conclude that data/message is secure during transmission and communication provides a secure channel between SCADA MTU and RTU. Current paper also achieved security services such as authentication, integrity, non-repudiation and confidentiality of data/message. At the end; paper implements the secure SCADA system within the cloud environment .In the future, current idea will implement in real environment/network and try to provide secure solutions related to SCADA protocols (such as DNP3, Modbus, and Fieldbus.) security. Current paper provides research direction to secure real time infrastructures and way to implement SCADA within cloud computing environments.

6. ACKNOWLEDGMENTS

I am sincerely and heartily grateful to my supervisor, Shahrulniza Musa, for the support and guidance he showed me throughout my research paper writing. I am sure it would have not been possible without his help. Besides I would like to thank to my parents and my friend, Irfan boosted me morally and provided me great information resources.

7. REFERENCES

[1] Systems Security http://www.wikinvest.com/concept/Cloud_Computing

[2] Keith Stouffer, Joe Falco and Karen Kent Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control, 2006.

[3] http://www.controleng.com/home/single-article/cloud-computing-for-scada/8a6ea192e6.html.

[4] Supervisory Control and Data

[5] Acquisition (SCADA) Systems, http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf

[6] Bonnie Zhu, Anthony Joseph and Shankar Sastry. "A Taxonomy of Cyber Attacks on SCADA Systems".

[7] Giovanni A. Cagalaban, Yohwan So and Seoksoo Kim, SCADA Network Insecurity: Securing Critical Infrastructures through SCADA Security Exploitation, December 31, 2009.

[8] Eric Conrad. Types of Cryptographic Attacks.

[9] Julian L. Rrushi." SCADA Intrusion Prevention System", March 14, 2006.

[10] Chapter 18: "Network Attack and Defense". Security Engineering: A Guide to Building Dependable Distributed Systems.

[11] Keith Stouffer, Joe Falco and Karen Scarfone. "Recommendations of the National Institute of Standards and Technology", June 2011.

[12] Eee Chuan Xu, Cheng Du and Xiangyue Kong. "An Application Layer DDoS Real-Time Detection Method in Flash Crowd", 2012 IACSIT Hong Kong Conferences.

[13] Ahsan Habib, Mohamed M. Hefeeda, and Bharat K. Bhargava, "Detecting Service Violations and DoS Attacks".

[14] N.Subramanian, University of Texas at Tyler, J.Z.Zalewski, S. D. Drager, William McKeever, Florida Gulf Coast University, AFRL/RITA, "Safe and Secure Integration of Automation Systems and Enterprise IT Infrastructure Using Cloud".

[15] Alcaraz, I.A , David Nu˜ ez, J. L, "Managing Incidents in Smart Grids a la Cloud Cristina".

[16] Geberslassie, M. and B. Bitzer, " Cloud Computing for Renewable Power Systems".

[17] "White Paper Cloud-Based SCADA Systems",The Benefits & Risks Is Moving Your SCADA System to the Cloud Right For Your Company.

[18] N.Subramanian, University of Texas at Tyler, J.Z.Zalewski, S. D. Drager, William McKeever, Florida Gulf Coast University, AFRL/RITA, Safe and Secure Integration of Automation Systems and Enterprise IT Infrastructure Using Cloud.

[19] P.Blomgren and S.M Kotronx. "Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan," American Gas Association (AGA), Draft 4, AGA Report 12, Mar.14.2006.

[20] S.C. Patel and G.D. Bhatt and J.H. Graham. "Improving the cyber security of Scada communication Network," Communication of ACM, Vol .52 No.7, July.2009.

[21] C. K. Kumar1, G. J.Arul Jose1, C. Sajeev1,C. Suyambulingom2, Safety Measures Against Man-In-The-Middle Attack In Key Exchange, 2006-2012 Asian Research Publishing Network (ARPN), VOL. 7, NO. 2, Feb 2012 ISSN 1819-6608.

[22] Robert Dawson, Colin Boyd , Ed Dawson ,Juan Manuel Gonz´alez Nieto, SKMA – A Key Management Architecture for SCADA Systems, Information Security Institute Queensland University of Technology, crpit.com/confpapers/CRPITV54Dawson.pdf.

[23] Hoon Ko, Application of Asymmetric-key Encryption Method for Internet-based SCADA Security, Journal of Security Engineering, 2008, www.sersc.org/journals/JSE/vol5_no6_2008/9.pdf

[24] Sugwon Hong, Seung-Jae Lee, Challenges and Perspectives in Security Measures for the SCADA System, ants.mju.ac.kr/publication/Chanllenges.pdf

[25] Martin Drahansky and Maricel Balitanas, Cipher for Internet-based Supervisory Control and Data Acquisition Architecture, Journal of Security Engineering, Jun 30, 2011, www.sersc.org/journals/JSE/vol8_no3_2011/1.pdf

[26] Osvaldo Gervasi, Encryption Scheme for Secured Communication of Web Based Control Systems, Journal of Security Engineering, Dec 31, 2010, www.sersc.org/journals/JSE/vol7_no6_2010/5.pdf

[27] Juan C. Asenjo, CISSP, Critical Aspects for Comprehensive SCADA Cyber Security,

Authentication, Encryption, and Seamless Key Management, www.docsharepoint.com/.../security%20and%20encryption/cri...

[28] DNPSec: Distributed Network Protocol Version 3 (DNP3) Security Framework, www.acsac.org/2005/techblitz/majdalawieh.pdf.

[29] Sandip C. Patel, Yingbing Yu, Analysis of SCADA Security Models, citeseerx.ist.psu.edu/viewdoc/download?...

[30] James H. Graham, Sandip C. Patel, Security Considerations in SCADA Communication Protocols, Sept 2004, Intelligent Systems Research Laboratory Technical Report TR-ISRL-04-01, www.cs.louisville.edu/facilities/.../ISRL-04-01.pd...

[31] Rosslin John Robles and Min-Kyu Choi, Symmetric-Key Encryption for Wireless Internet SCADA, Springer-Verlag Berlin Heidelberg, Communications in Computer and Information Science, Volume 58, 289-297, DOI: 10.1007/978-3-642-10847-1_36,2009, www.springerlink.com/index/ h87867t126455l11

[32] Ravindra Kumar Chahar, Goutam Datta, Navin Rajpal, Design of a New Security Protocol, International Conference on Computational Intelligence and Multimedia Applications 2007, www.cs.utexas.edu/~shmat/courses/cs395t_fall04/index.html

[33] Dr. E. Ramaraj, S. Karthikeyan and M. Hemalatha , A Design of Security Protocol using Hybrid Encryption Technique (AES- Rijndael and RSA), http://www.ijcim.th.org/past_editions/2009V17N1/p8-78-86 A%20Design%20of%20Security%20Protocol_using_HET-ijcimv17n1.pdf

[34] P. Prasithsangaree and P. Krishnamurthy, Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs,

http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1258477&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1258477

[35] Palanisamy, V. and Jeneba Mary, A, HYBRID CRYPTOGRAPHY BY THE IMPLEMENTATION OF RSA AND AES, International Journal of Current Research, Vol. 33, Issue, 4, pp.241-244, April, 2011, www.journalcra.com/?q=node/519

[36] http://www.controleng.com/home/single-article/cloud-computing-for-scada/8a6ea192e6.html.