Journal of Computer Science 10 (10): 2006-2019, 2014
ISSN: 1549-3636
© 2014 Science Publications
doi:10.3844/jcssp.2014.2006.2019 Published Online 10 (10) 2014 (http://www.thescipub.com/jcs.toc)

THE SECURITY SURVEY AND ANAYLSIS ON SUPERVISORY CONTROL AND DATA ACQUISITION COMMUNICATION

[1]Shahzad, A., [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 2014-01-15; Revised 2014-05-13; Accepted 2014-06-21

ABSTRACT

The SCADA system connectivity with several open networks using internet facility brought SCADA platform more vulnerable from attacks/threads. Therefore, the detail security review has been conducted, to find the potential security issues which are residing and warming the SCADA communication and also existing potential security solutions that are used to protect the SCADA communication. However, Security deployments are the future tread of this study. This security review is divided into four main sections: (1) Security Analysis for SCADA System, (2) SCADA Security using Cryptography Solution, (3) Key Management and Distribution Protocols for SCADA System and (4) SCADA Communication using Security Patterns. In this study; the SCADA security review has been conducted and generic security solution using cryptography will implement in future.

Keywords: Supervisory Control And Data Acquisition (SCADA) Systems, Security Review and Analysis

1. INTRODUCTION

1.1. Security Analysis for SCADA System

In this section, SCADA/Protocols connectivity with open networks or protocols and their security analysis has reviewed in detail from existing solutions or Implementations. This study is based on SCADA security issues such as SCADA/Protocols vulnerabilities, potential thread/attacks and other issues and also specifies recommendations for SCADA security enhancement such as intrusion detection system, firewall and DMZs implementation, security policies and thread/attacks analysis.

1.2. Technology Enhancement within SCADA System

"Supervisory Control and Data Acquisition (SCADA) systems" have been geographical distributed across different locations over the world using of Wide Area Network (WAN) technology. SCADA systems have been connected with numbers of remote terminal devices or PLCs through several types of networks such as LAN/WAN, protocols, transmission media such as wire/wireless. The enhancement within SCADA connectivity with several advance networks and uses of advance I.T infrastructures brought SCADA communication more demandable for end users. SCADA uses centralized station and controller thousand of remote terminal stations at the same time without limitation of networks and protocols. At the other side, highly/many interconnectivity of open standards networks, protocols and uses of open I.T infrastructure within SCADA system, made SCADA platform more vulnerable from several types of threads and attacks (Stouffer and Kent, 2006; NCSTIB, 2004).

SCADA system has several security weaknesses, whenever connected with open standard networks (protocols) that potential damage the communication (Fink and Wells, 2006). The most common vulnerabilities present within Communication (SCADA) including uses of Weak protocols, OS in-security, weak network setup, no viruses' protection, absent of cryptography protocol, weak password protection and

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

others are reviewed and basis on these vulnerabilities potential steps/requirements are specify to address the security and secure the SCADA communication including security policies for maintain security, uses of demilitarized zones or DMZs and firewalls, Intrusion detection and prevention system, security awareness, security assessments and risk management (2010).

1.3. Intrusion Detection within SCADA System

Pattern matching technique is uses to detect anomalies within SCADA communication. Network traffic using vector approach has been created and deviations method is uses to detect the anomalies. Several anomalies are detected with communication based on system abnormal behaviors. Current work review the several instruction detection approaches and proposed two intrusion detect solutions such as intrusion detection using signature and anomaly. Research is implemented in nuclear plant and intrusion detection solution is uses for intrusion detection during abnormal communication. The "Auto Associative Kernel Regression (AAKR) model" is uses for traffic observation by compare current state observation with previous state and the sequential probability ratio test or SPRT is hypothesis tester uses for testing AAKR model observations based on abnormal communication. Current work review the several intrusion detection approaches and implementation has been successfully detect several intrusions within SCADA communication. Usually inside communication; attacks are difficult to detect and the solution to check the behavior and performance impacts (in the case of intrusions) on SCADA system consider as future implementation (Jyothsna and Prasad, 2011; Singh, 2006).

Three major misconceptions are usually exist for SCADA security issues including SCADA implementation as standalone network, SCADA system is secure while connecting with other open networks, SCADA communication system has power to resist from attacks/threads and the vulnerabilities exist in SCADA including larger availability. For public users, no proper detection and prevention system and in security while connect with open networks. After detail review on SCADA security misconceptions and vulnerabilities, several terms/solution have been specify for SCADA security enhancement and resistance form attacks including connectivity awareness with other networks, communication with known stations, security evaluation for other networks, service access to authorized users, don't depend on vendors or proprietary protocols for system security , implement the existing security solution as part of vendor devices, strong authentication control over network, intrusion detection system implementation, perform audits related with SCADA components, review physical devices access and security, technique uses for attacks and vulnerabilities evaluation, assessments for potential vulnerabilities, expert security information system and security management system. Current work specifies the number of security awareness that significantly enhances the security of SCADA system and "energy management system or EMS" and overcomes the attacks by providing secure platform for communication (INL, 2008; Goetz *et al*., 2002; Amanullah and Zayegh, 2005).

1.4. SCADA Vulnerabilities, Potential Thread/Attacks and Recommendation

Potential cyber vulnerabilities have been review and security terms including data/information integrity, authentication and master/remote station security policies are specify to secure SCADA protocols communication and also uses of specific SCADA protocol based on system requirements (JNI, 2010; Kang and Robles, 2009) A testbed environment has been created for SCADA vulnerabilities testing and also addresses the attacks related with SCADA communication. Simulink platform from Mathworks (Matlab) is uses to complete developed the testbed system such as master/remote stations data exchange, data collection from sensors, communication network for data exchange and model for attack detection and prevention. This type of testbed is also known as "single simulation-based". "Federated simulation-based" uses many simulation platforms such as Omnet + + and DEVS to create testbed for several parts of system architecture. High-Level Architecture or HLA specify the platform for solving the coordination, session problems and data/information exchange within simulations (several) tools. While the "emulation/implementation "uses original vendors devices with their software implementations in real environment. These solutions generate accurate results as compare with other simulation based solutions and attacks within SCADA stations are analyzed and test in real (laboratory) environment (Giani *et al.*, 2008). Several attacks scenarios such as "denial of service attacks, integrity attacks, phishing attacks" are implemented to check the integrity and availability of SCADA communication between field devices and performance impacts on entire system (NSTB, 2009; Moore *et al*., 2001).

The "defense-in-depth" solution has been used to review the SCADA security issues, while SCADA connectivity with open network and protocols within electrical industry. Using of advance information technology with SCADA system is considered and provides solutions to minimized threads/attacks issues within communication (Beaver *et al*., 2002). The "client puzzles" technique has been uses to detect "SYN flood TCP DOS" within SCADA communication (when attacker again control on master controller resources) and also managed the session requirement within electrical industry uses QOS technique. Current work investigates the security (threads/attacks) within SCADA electrical industry communication and detects "SYN flood" DOS attack between master station and remote station (Bowen and Thomas, 2005; Coutinho *et al*., 2009).

A simulation environment has been implemented to analyze the thread/attack scenario with SCADA communication. Simulation environment has been implementing to detect the attacks and their effectiveness on SCADA communication (Wang *et al*., 2010; Fovino and Masera, 2010). SCADA system has several differences as comparison with traditional network (system) in the terms design and communication. SCADA system uses real time transmission devices, OS and protocols within communication, which are quite, differ from traditional networks such as LAN/WAN. The security parameters such data authentication, data integrity, data confidentiality, data availability and session management are more critical in real time infrastructure, rather than traditional networks. "4th DTTM technology" addresses the cyber security of SCADA system over internet. The current technology reviews the existing solutions and quantum cryptography uses to perform cryptographic operations and avoid the uses of cryptography solution such as RSA, AES and DES algorithms (Tuzzo, 2008).

Many organizations included "NERC, Federal Agency Regulatory Commission or FERC, Electric Reliability Organization or ERO, NIST" and others provide standards and solutions to secure SCADA system and address the cyber threads related with communication and some of SCADA vendors also try to putting security mechanism within protocols. "North American Electric Reliability Corporation or NERC, Critical Infrastructure Protection or CIP" specified standards frameworks for cyber security detection or identification and security protection and some of main requirement such as intrusion detection, user logs and security issues, audits for data fetching and storage, authenticity and authorization between devices, log access to ESP, tools to protection from malicious attacks, mechanism to handle critical events, security tools updating and upgrading, stronger password (length) and availability of resources on access. SCADA IEC 62351 standard specify the end-to-end authentication and integrity mechanisms using of hash function. Data /information are exchange securely between the field devices and in case of attacks/thread message are discarded and response will reply back to sender (Farkhod and Kim, 2010). The IEC 62351 authentication mechanism uses cryptography keys such as asymmetric and symmetric and PKI and digital signature uses asymmetric for computation. Transport Layer Security (TLS) provides strong security mechanism for TCP/IP protocol and running below then application level protocols. SCADA protocol provides end-to-end encryption for applications running over Transport Layer Security (TLS), while IPSec provides encryption and other security mechanisms between connected routers. SCADA uses cryptography solutions to provide "security services such as authentication, integrity, non-repudiation and confidentiality" to secure SCADA protocols communication end-to-end. Without implementation of these security services SCADA /protocols communication is unsecure. Cryptography is a stronger security solution for SCADA system and other security mechanisms such as DMZ, firewall, IP sec and intrusion detection systems are also commonly uses for SCADA security. A current paper reviews the SCADA cyber security issues in detail and then specifies several security solutions for SCADA security enhancement (Cleveland, 2006; Farkhod and Kim, 2010).

Some progress has done to resolve the issues related with SCADA security. Several international or organization s such as "Instrumentation, Systems and Automation society (ISA)/International Electrotechnical Commission (IEC), Institute of Electrical and Electronic Engineers (IEEE), Government Accountability Office (GAO), National Institute of Standards and Technology (NIST), System Protection Profile for Industrial Control Systems (SPPICS), Federal Information Processing Standards, National Infrastructure Security Co-ordination Centre (NISCC) and Cisco System" and protocol organization such as "DNP3, modbus/TCP and field bus", are try to designing the solutions for protecting/securely the SCADA communication. Current paper review the SCADA security issues in detail and then gives some solutions/treads for SCADA protection such as "Artificial Immune Algorithm" for intrusion detection and prevention," tree model " for cyber attacks, security model for field devices, Model for vulnerabilities evaluation. Papa briefly discuses the security issues detail with SCADA communication and difference related with corporate/traditional networks and SCADA networks. Also give some research directions for SCADA security (Ma *et al*., 2012; Cai *et al*., 2008; Cristina *et al*., 2012). SCADA system vendors and developer have been only focusing on functional parts of SCADA System (SCADA and protocols) such scalability, reliability, performance and access without security consideration in mind. There is no solution that fulfills the requirements of SCADA system security. All SACAD functional performances are depending on security issues, if SCADA system is fully secure then functionalities automatically achieved (Rautmare, 2011; INL, 2008). Current work also analysis some security treads such as connectivity with other interfaces and open protocols and open connection with internet and vulnerabilities such as insecure information, insecure control station, insecure SCADA architecture, insecure network communication and insecure SCADA platform (Stamp and Young, 2003). Paper gives detail concept of SCADA architecture and configuration such as purposes of SCADA system, SCADA main parts (master station, remote station and Human Machine Interface or (HMI), SCADA architecture and SCADA communication network and most important the security issues and at the end, gives some recommendation for security enhancement such as Criteria for SCADA security, best approach to handle vulnerabilities, limited network connectivity, security audit, security policies, solution for configuration and management , security Awareness solution (program) and solution for disaster event (Stamp *et al*., 2003; Rautmare, 2011).

Several vulnerabilities have been review for SCADA protection from cyber attacks/thread. The Paper provides major misconceptions within SCADA communication, which creates vulnerable platform for SCADA communication (RIPTECH Inc., 2001; Hadbah *et al*., 2008). Most common misconceptions such as SCADA standalone network (physical network), SCADA network become secure with corporative networks and attacker impossible to access SCADA communication and vulnerabilities such as open access and Availability, no protection/security mechanism, no proper configuration, open Network users, no firewalls and DMZs implementation, no enhance audit(information) system and lack of intrusion detection and prevention system. Basis on above misconception and vulnerabilities; current work also specify the several major recommendation for SCADA security such as time to time security Assessments, implementation of firewalls and DMZs, security policies, strong information system security and strong intrusion detection and prevention system. "RIPTECH" provides several security Services for real time infrastructure (SCADA) (Hong and Lee, 2010). "RIPTECH" platform is able to handle larger amount of data/information from number of field devices and provide security on identifying the threads during transmission and provides services such as security assessment, security auditing and policies for security management and security (threads) testing tools. Several SCADA system (within networks and protocols) vulnerabilities are review and threads scenario have been created, which are mostly commonly found within SCADA communication such as buffer overflow, SQL Injection, UDP port (attack), data spoofing, Chain/Loop Attack, SYN flood, DNS forgery and also specify attacks present within protocols such as TCP/IP, ICCP and MMS protocol (Fovino and Masera, 2010; Zhu *et al*., 2011).

2. SCADA SECURITY USING CRYPTOGRAPHY SOLUTION

This section is sub divided into five main parts: (1) Cryptography approach Analysis for SCADA system, (2) Cryptography implementations for SCADA system, (3) Cryptography implementations for SCADA Protocols, (4) Cryptography Implementation and SCADA Cyber Security and (5) Cryptography implementation for wireless SCADA System.

2.1. Cryptography Approach Analysis for SCADA System

American Gas Association (AGA) has been review detail literature related with American security for critical systems Industrial Control System or (ICS) such as electrical industry, water/wastes water management and controlling industry, gas association and other and also included attack/threads and hacker interaction within communication, which were demobilizing the ICS communication infrastructure. During SCADA communication between networks (field devices) minimized the operational session for handler (operators) and based on comprehensive review related with SCADA threads and vulnerabilities and solution/method to secure SCADA communication infrastructure included uses of security requirements and policies for communication (request/response) and ways/procedures for field devices testing. Several approaches were indentify for SCADA protection from cyber attacks/threads and also test SCADA security using End Date 5 Asymmetric key algorithms such as RSA and Digital Signature Algorithm (DSA) have been uses to securing SCADA communication (End-to-End) connected over internet (LAN/WAN). The proposed algorithms are very famous asymmetric algorithm with secure implementation results within communication. Implementation results concluded that , impossible for attacker to gain access over SCADA communication connected with internet and security feature such as authentication and confidentiality of data have been achieve during communication between master station cryptography, this approach is difficult to developed but bases results are more accurate than other appropriate techniques (AGA, 2006). AGA series part3 specify the solution (cryptography) to protect the SCADA system, connected with high speed networks with field devices intercommunication. While, AGA series (part4) specify the solution to protect/secure SCADA system at the time of developing (manufacturing). Cost factor will decrease and security protection (performance) will significantly enhance during SCADA parts/components manufacturing. More advances, intrusion detection system, policies for communication security enhancement, large SCADA system operations support and information/data protection will AGA series future considerations (Hadley and Edgar, 2007). American Gas Association (AGA) series define solutions for SCADA security, specifically to secure SCADA system communication from cyber threads/attacks and specify requirement for end user system integration with AGA series and cyber security protection related with them. AGA series successfully test the end user communication needs include hard ware, software and other and provide secure platform protection from security (cyber security) (Rush *et al*., 2006).

The implementation of “retrofit solutions” that addresses the SCADA cyber security become major concerned for critical infrastructure such as “American Gas Association (AGA-12) standard, North American Electric Reliability Council (NERC), Gas Technology Institute (GTI) and the Instrumentation Systems and Automation Society (ISA). These solutions perform main roles in SCADA communication included minimize security (cyber security) and make field devices always available for operations. The implementation of “cryptography retrofit solutions” within SCADA communication become “bump in the wire” that has developed without distributing the SCADA infrastructure and performance or operations. These solution are usually developed between master station and remote stations or/and remote stations and master station as part of SCADA communication. Usage of cryptography solutions within SCADA communication, the feature such as Data/message authentication, confidentially, integrity and non repudiation are successfully achieved and significant increases the security/protection from attacks/thread (cyber) that mitigating SCADA communication. Current article also provides review, based on SCADA configuration, development and operations, SCADA protocols specifications and operations, key management and distribution between field devices, cyber risk and “Role Based Access Control (RBAC)” solution, (Hong *et al*., 2010).

2.2. Cryptography Implementations for SCADA System

The master station initials the communication with remote station within SCADA network. The master station calculates the hash digest of required message/data that being transmitted to remote station and when hashing process will complete and then hash digest is encrypted using private key “authentication Octets “solution. At the other end; remote station uses public key of master station and decrypt the hash digest value. Message hashing function is perform again at remote station and hash digest value is compare between master station hash digest and remote station hash digest. When hash digest values are match then remote station specify that message is coming from secure authentication source and message is not change during communication. Same results will achieved when digital signature will perform from remoter station to master station and successfully data/message authentication and integrity function performed. During master station/remote stations communication; message is not encrypted to save the session related with encryption/decryption process. Two security solutions such as “Wrap SCADA protocols” base on SSL/TSL and IP security and “Cryptography solutions for enhance SCADA protocols” have been specified with limitation of cryptography solution such as SSL/TSL protocols are based on TCP for communication (reliable protocol) and cryptography for security purposes (Patel *et al*., 2009). Patel and Graham (2006), new cryptography solution has been implemented for internet base SCADA system and formal methods are uses to verify the proposed implementation.

Asymmetric key algorithms such as RSA and Digital Signature Algorithm (DSA) have been uses to securing SCADA communication (End-to-End) connected over internet using LAN/WAN. The proposed algorithms are very famous asymmetric algorithm with secure implementation results within communication. Implementation results concluded that , impossible for attacker to gain access over SCADA communication connected with internet and security feature such as authentication and confidentiality of data have been achieve during communication between master station remote stations or/and remote station and master station (Ko, 2008). Message/data has been encrypted by using symmetric algorithm Advance Encryption Standard or (AES) and symmetric key encrypted by public key of receiver using asymmetric algorithm Elliptic Curve Cryptography or (ECC) and then data integrity function has been achieved by MD5 hashing algorithm. Current solution successfully implemented and addresses the "security services such as data confidentiality, data authentication, data integrity and non-repudiation function" between SCADA communication between master controller and remote stations/field devices. Paper also review the weakness related with asymmetric and symmetric solutions and propose a hybrid solution to secure SCADA communication (Drahansky and Balitanas, 2011). A hybrid solution, which has been based on "Extensible Authentication Protocol (EAP) and Kerberos protocol" (Aboba and Eronen, 2008) and provides authentication and authorization mechanisms at each end of system communication or between master station and remote station or/and remote station and master station and protect/secure the Control System (CS) without any performance impacts (Manz *et al*., 2010). The security model has been implemented within SCADA communication network, after detail review on threads and vulnerabilities analysis. The major threads found within SCADA communication are open IDSs, modification, spoofing, man-in-the-middle, non-repudiation, replay attack and eavesdropping attacks and major vulnerabilities are no IDSs, security policies, no audits system, no backup on disaster and open network connections. Basis on above threads and vulnerabilities two solutions are implemented to resolve the SCADA security issues. In first solution, hash value is calculated for message being sent to remote station. When hash digest is calculated successfully then private key is uses to encrypt the hash digest as digital signature (Shahzad *et al*., 2014). At the other end; remote station received the digital signature and decrypt the digital signature using master station public.

On successful decryption; remote station again calculate the hash value for message and compare with master hash digest value. If the values match with each other, than remote station specify that message is authentic and during transmission message bytes are not change. If the attacker, get public key of master station than he uses same key to decrypt the hash digest because message was not encrypted it's self, to save time (session).

However, this is not possible for attacker to gain access on communication because he only get public key of master station. When he try to encrypted the hash digest to change the information before sending to remote station but this could not possible for attacker because he has no proper(authentic) private key. If he send the message without using of master private key, upon receiving , when remote station try to decrypted the message than impossible to decrypt because message need master station public and private key to decrypt the desire message. Remote station verifies that message is not authentic. RTU also conclude that transmission time of master station is not same as receiving time. In another solution; message authentication is perform secretly and only know by sender/receiver. Each time challenge is change but must be unique. Upon response, message (having unique identifier) is passing to hash function with added secret key. This is not possible for attacker to gain access on message because every time challenge (request) is unique. This type of authentication is used for reply attack prevention (Patel and Yu, 2007).

2.3. Cryptography Implementations for SCADA Protocols

Cryptography solution has been implemented within SCADA/DNP3 communication using AES (symmetric algorithm) and SHA-1 algorithm and successfully archived the "security services such as authentication, confidentiality and integrity". In second phase, Hybrid cryptography solution using AES, RSA and SHA-1 algorithm has been implemented within "application layer and data link layer" of DNP3 protocol and the "security services such as authentication, confidentiality, integrity and non-repudiation", have been also successfully archived. Number of attacks such as authentication attacks, confidentiality attacks, integrity attacks and non-repudiation attacks are lunched using built-in tools as attacker and performance results are measured within normal and abnormal traffic (Musa *et al*., 2013a; 2013b).

Several cryptography solutions have been analysis and specified for SCADA/DNP3 communication. These all solution is based on SCADA/DNP3 security enhancement during communication between master station and remote station. Another research, hybrid cryptography has been implementing within cloud computing environment. First entire SCADA/DNP3 system is deployed within cloud computing environment and then security has been tested using hybrid solution (AES, RSA and hashing algorithms) (Shahzad *et al*., 2013; DNP3, 2011). Authentication solution has been specifying for SCADA/DNP 3 protocol using Message Authentication Code or HMAC algorithm. Paper review the security related with SCADA/DNP3 protocol and the associated processes (operations) for communication. HMAC algorithm has been uses to calculate the hash value (same as CRC technique) of message being transmitted to receiver (challenger) (CSE-SemaPhore, 2012; Kang and Robles, 2009). Hash value successfully calculated and sent to receiver from stations. At the other end, receiver (challenger) uses again the HMAC solution to perform hashing on message and when hashing will complete the values are comparing from sender and receiver. If message is critical then dummy bytes (message) will response and if several times receiver receives critical messages then challenger recognize that attacker is intercepting the communication. In non critical state, challengers specify that message is coming from secure source and message (bytes) is not change during transmission and attacker is not intercepting the communication between stations. The threads such as spoofing, data modification, data replay, Eavesdropping and non-repudiation function are successfully addresses in current proposed work and principles/ways are consider for SCADA/DNP3 security including authentication without encryption, Application layer security, communication solution between master to remote station or/and remote to master station, challenge/response solution, Shared Keys solution, Tolerance solution, updating and broadcast solution (Gilchrist, 2008). Many SCADA vendors have been implementing security standards/solutions to secure/protect SCADA/DNP3 and other SCADA protocols communication (Evans and Bement, 2008; UCI, 2012).

Another research, "SCADA Cryptographic module or SCM" as part of "American Gas Association AGA 12-2 Standard"; uses as encryption/decryption solution for SCADA protocols security including distributed network protocol or DNP3 and modbus. The proposed solution will implement/integrated within and as external device solution to secure SCADA communication and also know as called "bump-in-the-wire". Based on external solution, security has been develop in existing SCADA communication and key algorithm is uses for message encryption as part of SCM and keys are shared between communication stations. A layer called "wrapper layer" is provided by SCM and also manage the SCADA communication time and keys distribution between field devices. Secret keys are uses to provide authentication between devices communication, while dynamic key is uses to mange time during encryption. When session is expire then new session key will generated and uses for encryption and signature processes (West, 2008). At the end, remote station uses SCM to open cipher text of message and calculated signature (sender or master station) from "wrapper layer protocol" because master cipher text and signature (sender or master station are encapsulated within "wrapper layer protocol". Remote station again calculates the signature value and then compare with sender signature. If the signature values match then cipher message is decrypted using session key and plain text is found (recover from cipher text). Several characteristics include master/remote station architecture, each field device security within network, security implementation over low embedded device, bandwidth uses (low), CA non accessible, problem to sent lager amount of data, insecure network (venerable), session management and system upgrading, are consider by SCM for addressing SCADA security issues As conclusion, proposed solution is implemented between SCADA communications (sender/receiver) and significantly secures the communication and also addresses the attacks/threads that provide vulnerable platform for SCADA system (Bhattacharyya, 2008; West, 2008).

The 34 bytes security structure having 5 fields has been proposed in replacement of Cyclic Redundancy Checker (CRC) bytes within data link layer. CRC have 34 bytes within data link layer of DNP3 and uses for error detection during communication between SCADA master and remote stations. Current work has been reviewed the existing security/research solutions and major attacks that creates vulnerable platform for SCADA communication. Several attacks scenarios have been discussed related with communication, when attacker attack and cryptography solutions have been proposed for SCADA security without uses of specific algorithms (Asymmetric or symmetric).

SCADA security review from existing researches and conceptual solutions (uses of cryptography) for the purposes of security services have been proposed with real implementation as future research treads (work) (Majdalawieh *et al*., 2006). Chandia *et al*. (2007), two solutions are specified and implemented in Modbus protocol. First solution; uses security services to decrease the time (performance) according to real infrastructure standard and second solution; uses system (forensic) to collect the data (traffic) within SCADA network then made analysis and provides security for SCADA system and increase performance by monitoring SCADA communication.

2.4. Cryptography Implementation and SCADA Cyber Security

SCADA connectivity with several Networks (LAN/WAN) using internet facility brought SCADA platform more vulnerable from communication attacks (cyber attacks). Several existing solutions have been developed for securing SCADA communication but current solution uses encryption method to secure SCADA communication. SCADA network traffic is increase while applying encryption solution but significance security will achieve within SCADA communication and performance issues (traffic load with session) are consider during encryption process. Quality of Service (QOS) method has been used to balance SCADA network traffic load with the calculation of key distribution session between nodes and encryption techniques using Symmetric and Asymmetric have generally discusses to protect SCADA communication from cyber attacks (Kang and Kim, 2007a).

Web security is one of the major issues related with SCADA system. Traditional SCADA system has been connected with limited networks “such as Local Area Network (LAN)” and small private networks but currently SCADA systems are connected with several open standards networks (protocols). SCADA connectivity with several open network brought SCADA communication more vulnerable from cyber/web attacks. After detail review related with web SCADA system “Crossed Cryptography solution” has been proposed to secure SCADA communication. Cryptography algorithms such asymmetric and symmetric have been analysis in detail and a solution has been proposed that is based on both asymmetric and symmetric cryptography algorithms for better performance. SCADA master station initial the communication with remote station. The message/data being transmitted from master station is encrypted with Advance Encryption Standard (AES) algorithm as part of symmetric cryptography and then AES key is encrypted by using ECC algorithm as part of asymmetric cryptography. When encryption process is completed than encrypted message and encrypted key is sent to SCADA remote station along with message hash digest. At the receiving end, message hash digest is calculated again to compare with mater hash digest. If hash digests values match successfully then remote station verify that message is coming from authentication source and message value not change during transmission. Data/message authentication, confidentially, integrity and non repudiation security services also have been achieved to meet the SCADA security requirements. Paper also highlights the SCADA web security issues and cryptography using asymmetric and symmetric advantages/disadvantages over web (Gervas, 2010; Subasree and Sakthivel, 2010; Chahar *et al*., 2007).

2.5. Cryptography Implementation for Wireless SCADA System

Hybrid cryptography using AES and RSA algorithms has been implemented for SCADA communication between field devices within wireless environment. SCADA nodes are connected with each other using wireless router. Message encryption/decryption performances results have been measured during communication and security services are also verified upon receiving message c. A symmetric cryptography solution has been proposed to secure the SCADA system connected with wireless networks. Using wireless networks, SCADA system significantly decrease the cost factor as compare with wire networks but brought several security issues for SCADA communication, So, RC4 algorithm has been developed to overcome these security issues related with SCADA with wireless network (James and Patel, 2004). Symmetric solution is a part of cryptography algorithm and uses same key for message/data encryption/decryption process. Symmetric key is shared between master and remote station using secure link/channel. Symmetric cryptography algorithm is based on stream cipher and block cipher and RC4 algorithm is also a stream cipher with variable key length for encryption/decryption process. RC4 algorithm is based on random permutation and mostly developed in SSL and WEP. RC4 has number of advantages including simple implementation and fast speed and disadvantages including not specify for new applications (systems) and security flaws within WEP, RC4 avoid the used of linear register and focus on message (bytes) interpretation. Proposed work successful deployed between SCADA master station and remote station or/and remote station and master station using wireless communication. WEP uses RC4 algorithm data/message confidentiality and CRC for data/message integrity (Robles and Choi, 2009).

3. KEY MANAGEMENT AND DISTRIBUTION PROTOCOL FOR SCADA SYSTEM

Cryptography (Symmetric and Asymmetric) key management solution has been implemented within SCADA communication between master and remote stations, before detail review on SCADA security issues and related vulnerabilities. The proposed solution "A Key Management Architecture for SCADA Systems (SKMA)" has been developed between master and remote communication and in the case of multiple master stations connected with single remote station; keys are manually installed and configured. The implementation is twofold, "A Key Management Architecture for SCADA Systems (SKMA)" specify the detail solution for keys distributions and configuration process for secure SCADA communication based on cryptography (symmetric and Asymmetric) and other solution "Secure Key Management Protocol (SKMP)" provide mechanism/methods to secure SCADA (keys distribution to/from key distribution center or KDS) communication based on existing security methods and ISO standard is uses for long key session generation process between SCADA Stations. The keys distribution processes between stations are securely distributed and security terms included data integrity, availability and confidentiality for SCADA system are also highlighted generally (Dawson *et al*., 2006). Master station initial the communication with remote station using of symmetric key algorithm. Symmetric key has been uses secure channel for key distribution process between stations without using of Key Distribution Center (KDS). Symmetric method has been uses to check the security performance and also specify the policies for key distribution between nodes, Formal mathematical methods for SCADA security and the uses of symmetric algorithms are future topic of current research (Kang and Kim, 2007b). Multicasting approach for key distribution and management is new approach within SCADA systems, which significantly reduces the cost and provides better performance from existing solutions (Choi *et al*., 2010).

A new key management solution has been implemented for purposes of securing SCADA communication between master station and remotes nodes (stations). After conducting detail review related with SCADA security and the existing key management and distribution solutions or/and protocols, two solution have been proposed. First solution is based on SCADA communication security (master/remote stations) by implementing new architecture for key management between nodes or message broadcast from master station to remote stations within SCADA networks and second is based on SCADA performance included total session computation between SCADA nodes during communication between master station and remote stations. The paper also high light the basic requirement for SCADA security such as data Confidentiality, data integrity, Demilitarized Zone, firewall, data Availability, Access Control, Security for Networks Policies for communication Security. Securely key broadcasting and key management (session expire and update key) (Lee *et al*., 2009). An advance key management solution is implemented based on multicast communication to improve the computation performance between remote stations or field devices connected with SCADA master controller. Current solution has been develop based on number of drawbacks within existing research done such "Advanced Key Management Architecture for Secure SCADA Communication, Key establishment for SCADA Systems (SKE) and Key management scheme for SCADA systems (SKMA)" (Choi *et al*., 2009; Xiao *et al*., 2010).

Message authentication code has been used to secure the communication (or distribution automation system or DAS) between field devices after conducting detail review on cyber attack/threads and avoid the encryption solutions; because of complex computation. Also uses symmetric algorithm for key distribution and avoid asymmetric algorithm because the public key encryption use multiple keys for message/data security. The article highlighted the requirements that have been uses for SCADA communication and conduction detail review on SCADA security issues related with cryptography key management from existing works done by researchers included Key-server based, Point-to-point architectures, Standard PKI, "Customized" PKI, TC57WG15 work and choices-IEC62351, "DNP3 User Group-Secure DNP3 v1.0", The IEEE P1689 draft, Smart meters initiatives and also discuss Challenges, issues, technical perspectives and results based on existing key management implementations (NSTB, 2009; Moore *et al*., 2001).

4. SCADA COMMUNICATION USING SECURITY PATTERNS

Security pattern is a tools uses for SCADA communication security and addresses the potential attacks/threads which warm the SCADA system. Several patterns are specified and uses with other pattern to secure SCADA architecture included master station security, remote station and SCADA network or communication. At controller stations side; the physical attack is overcome by uses of "role-based access control or RBAC pattern with combination of authenticator and logger patterns and authorization pattern" with combination of authenticator and logger patterns uses for attacks such as malicious attack, wrong commands, malicious attack with runtime parameters and "firewall pattern with an intrusion detection system or IDS pattern" are used for denial of service attacks. At remote stations side; the physical attack is overcome by uses of "role-based access control or RBAC pattern with combination of authenticator and logger patterns" and authorization pattern with combination of authenticator and logger patterns used for attacks such as malicious attack field stations, wrong commands, malicious attack with runtime parameters and "firewall pattern with an intrusion detection system or IDS pattern" are used for denial of service attacks. Communication network attacks such as sniffing is handle by using cryptography solutions, spoofing and DOS by using authentication pattern message is during communication between master and remote or field station (Fernandez and Larrondo-Petrie, 2010). Several security patterns are specify for SCADA security or secure SCADA architecture and deployed in different parts of SCADA system to address the attack/threads which warm the communication. The proposed work review the SCADA architecture and threads related with SCADA system components including master station attacks, remote station attacks and network communication attacks. Security pattern solution is uses as tool to addresses these threads and secure SCADA communication long run and uses Unified Modeling Language (UML) solution including class diagram and sequence diagram for implementation. Security pattern are also uses for Secure system analysis and construction and evaluation for system security (Fernandez *et al*., 2009).

5. METHODOLOGY

In this research; detail SCADA security review has been conducted, to find the potential vulnerabilities, threads/attacks and other security issues that are linked with SCADA system communication. After conducting the security analysis; generic security solution using cryptography algorithms is suggest, that securing the communication of SCADA system as a part of Industrial Control System (ICS). The main steps that are related with research methodology are illustrated in **Fig. 1**.

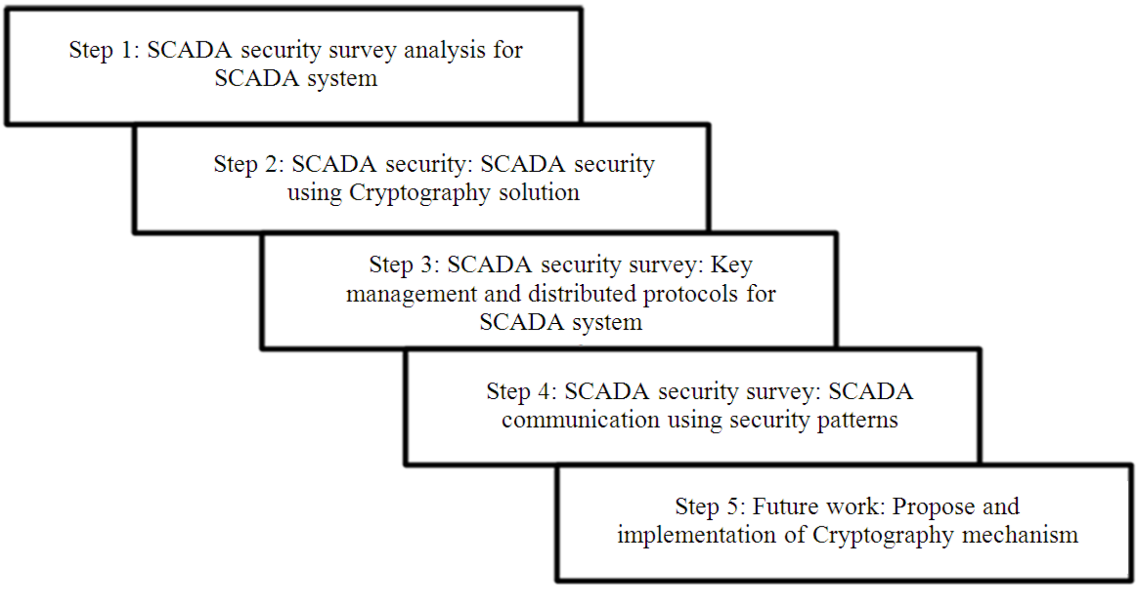
Step 1: SCADA security survey analysis for SCADA system
Step 2: SCADA security: SCADA security using Cryptography solution
Step 3: SCADA security survey: Key management and distributed protocols for SCADA system
Step 4: SCADA security survey: SCADA communication using security patterns
Step 5: Future work: Propose and implementation of Cryptography mechanism

Fig.1. Proposed Research methodology

6. CONCLUSION

The detail literature has been conducted which is based on SCADA existing implementations or security implementations and security issues such as SCADA/protocols system vulnerabilities, potential thread/attacks and other issues. Several recommendations and security methods are specified for SCADA security enhancement. However, the overall study scope is limited to SCADA system and its protocols security analysis. In future work; based on current review, security using cryptography methods will deploy within SCADA multicasting and broadcasting transmissions.

7. ACKNOWLEDGMENT

I would like to thank to my parents and my friend, M. Irfan boosted me morally and provided me great information resources.

8. REFERENCES

Aboba, D. and P. Eronen, 2008. Extensible Authentication Protocol (EAP) key management framework. Network Working Group.

AGA, 2006. Cryptographic Protection of SCADA communications. Part1: Backgroud Policies and Test Plan.

Amanullah, M. and A. Zayegh, 2005. Network Security Vulnerabilities in SCADA and EMS. Proceedings of the Asia and Pacific Transmission and Distribution Conference and Exhibition, (DCE ‘05), Dalian, pp: 1-6. DOI: 10.1109/TDC.2005.1546981

Beaver, D., W.D. NeuMann and M.D. Torgerson, 2002. Key management for SCADA. Sandia National Laboratories, Sand Report.

Bhattacharyya, D., 2008. The taxonomy of advanced SCADA communication protocols. J. Security Eng., 5: 517-526.

Bowen, T. and R.W. Thomas, 2005. A Plan for SCADA security to deter dos attacks. Proceedings of the R&D Partnering Conference Department of Homeland Security, (DHS ‘05).

Cai, N., J. Wang and X. Yu, 2008. SCADA system security: Complexity, history and new developments. Proceedings of the 6th IEEE International Conference on Industrial Informatics, Jul. 13-16, IEEE Xplore Press, Daejeon, pp: 569-574. DOI: 10.1109/INDIN.2008.4618165

Chahar, R.K., G. Datta and N. Rajpal, 2007. Design of a new security protocol. Proceedings of the International Conference on Computational Intelligence and Multimedia Applications, Dec. 13-15, IEEE Xplore Press, Sivakasi, Tamil Nadu, pp: 132-136. DOI: 10.1109/ICCIMA.2007.147

Chandia, R., J. Gonzalez, T. Kilpatrick, M. Papa and S. Shenoi *et al*., 2007. Security Strategies for SCADA Networks. Proceedings of the IFIP International Federation for Information Processing, (FIP’ 07), Springer US, pp: 117-131. DOI: 10.1007/978-0-387-75462-8_9

Choi, D., H. Kim, D. Won and S. Kim, 2009. Advanced key-management architecture for secure SCADA communications. IEEE Tran. Power Delivery, 24: 1154-1163. DOI: 10.1109/TPWRD.2008.2005683

Choi, D., S. Lee, D. Won and S. Kim, 2010. Efficient secure group communications for SCADA. IEEE Trans. Power Delivery, 25: 714-722. DOI: 10.1109/TPWRD.2009.2036181

Cleveland, F., 2006. IEC TC57 Security Standards for the power system's information infrastructure-beyond simple encryption. Proceedings of the EEE PES Transmission and Distribution Conference and Exhibition, May 21-24, IEEE Xplore Press, Dallas, TX, pp: 1079-1087. DOI: 10.1109/TDC.2006.1668652

Coutinho, M., D. Silva, L.E.B, Martins, H.G. Lazarek and H. Neto *et al*., 2009. Anomaly detection in power system control center critical infrastructures using rough classification algorithm. Proceedings of the 3rd IEEE International Conference on Digital Ecosystems and Technologies, Jun. 1-3, IEEE Xplore Press, Istanbul, pp: 733-738. DOI: 10.1109/DEST.2009.5276789

Cristina, A., G. Fernandez and F. Carvajal, 2012. Security aspects of SCADA and DCS environments. Proceedings of the Lecture Notes in Computer Science Critical Infrastructure Protection, (CIP ‘12), pp: 120-149. DOI: 10.1007/978-3-642-28920-0_7

CSE-SemaPhore, 2012. Implementation of DNP3 secure authentication, case. Copyright SemaPhore.

Dawson, C., E. Dawson, J. Manuel and G. Nieto, 2006. SKMA: A key management architecture for SCADA systems. Proceedings of the Australasian Workshops on Grid Computing and E-Research, (CER’ 06), ACM, Inc. Darlinghurst, pp: 183-192.

DNP3, 2011. DNP3 Secure authentication version 5 (SAv5).

Drahansky and M. Balitanas, 2011. Cipher for internet-based supervisory control and data acquisition architecture. J. Sec. Eng., 8: 337-337.

Evans, P. and A.L. Bement, 2008. The keyed-Hash Message Authentication Code (HMAC). 1st Edn., FIPS Publication, pp: 198.

Farkhod, A. and T. Kim, 2010. Research trend on secure SCADA network technology and methods. Tran. Syst. Control, 5: 635-645.

Fernandez, E.B. and M.M. Larrondo-Petrie, 2010. Designing secure SCADA systems using security patterns. Proceedings of the 43rd Hawaii International Conference on, System Sciences, Jan. 5-8, IEEE Xplore Press, Honolulu, HI, pp: 1-8. DOI: 10.1109/HICSS.2010.139

Fernandez, E.B., J. Wu, M.M. Larrondo-Petrie and Y. Shao, 2009. On building secure SCADA systems using security patterns. Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, Apr. 13-15, New York. DOI: 10.1145/1558607.1558627

Fink, D. and R.A. Wells, 2006. Lessons learned from cyber security assessments of SCADA and energy management systems. NSTB.

Fovino, A. and M. Masera, 2010. Taxonomy of Security Solutions for the SCADA Sector, Security of Critical Networked Infrastructures (SCNI) Action, JRC-Joint Research Centre of the European Commission, Version 1.1.

Gervas, O., 2010. Encryption scheme for secured communication of web based control systems. J. Security Eng., 6: 609-618.

Giani, G., T. Roosta, A. Shah, B. Sinopoli and J. Wiley *et al*., 2008. A testbed for secure and robust scada systems. Proceedings of the 14th IEEE Real-Time and Embedded Technology and Applications Symposium, (RTAS ‘08), New York. DOI: 10.1145/1399583.1399587

Gilchrist, G., 2008. Secure authentication for DNP3. Proceedings of the 21st Century Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy, Jul. 20-24, IEEE Xplore Press, Pittsburgh, PA., pp: 1-3. DOI: 10.1109/PES.2008.4596147

Goetz, G., E. Byres, T. Gannon, R. Gray and D. Stempfley *et al*., 2002. Cyber security of the electric power industry, Investigative Research for Infrastructure Assurance (IRIA) group- institute for security technology studies.

Hadbah, A., A. Kalam and H. Al-Khalidi, 2008. The subsequent security problems attributable to increasing interconnectivity of SCADA systems. Proceedings of the Australasian Universities Power Engineering Conference, Dec. 14-17, IEEE Xplore Press, Sydney, NSW., pp: 1-4.

Hadley, K. and T.W. Edgar, 2007. AGA-12, Part 2 Performance Test Results.

Hong, S. and M. Lee, 2010, Challenges and direction toward secure communication in the SCADA System. Proceedings of the 8th Annual Communication Networks and Services Research Conference, May 11-14, IEEE Xplore Press, Montreal, QC, Canada, pp: 381-386. DOI: 10.1109/CNSR.2010.52

Hong, S., M. Lee and D.Y. Shin, 2010. Experiments for embedded protection device for secure SCADA communication. Proceedings of the Asia-Pacific Power and Energy Engineering Conference, Mar. 28-31, IEEE Xplore Press, Chengdu, pp: 1-4. DOI: 10.1109/APPEEC.2010.5448606

INL, 2008. Common cyber security vulnerabilities observed in control system assessments by the INL NSTB Program, U.S Department of Energy, Idaho National Laboratory.

JNI, 2010. Architecture for secure SCADA and distributed control system networks. White Paper.

James, H.G. and S.C. Patel, 2004. Security considerations in SCADA communication protocols. Intelligent Syst. Res. Laboratory Technical Report TR-ISRL-04-01.

Jyothsna, V., R.V.V. Prasad and K.M. Prasad, 2011. A review of anomaly based intrusion detection systems. Int. J. Comput. Applic., 28: 26-35. DOI: 10.5120/3399-4730

Kang, D.J. and R. J. Robles, 2009. Compartmentalization of protocols in SCADA communication. Int. J. Advanced Sci. Technol., 8: 27-36

Kang, D.J. and H.M. Kim, 2007a. A method for determination of key distribution period using QoS function. Proceedings of the Future Generation Communication and Networking, Dec. 6-8, IEEE Xplore Press, Jeju, pp: 532-535. DOI: 10.1109/FGCN.2007.17

Kang, D.J. and H.M. Kim, 2007b. A proposal for key policy of symmetric encryption application to cyber security of KEPCO SCADA network. Proceedings of the Future Generation Communication and Networking, Dec. 6-8, IEEE Xplore Press, Jeju, pp: 609-613. DOI: 10.1109/FGCN.2007.36

Ko, H., 2008. Application of asymmetric-key encryption method for internet-based SCADA security. J. Security Eng., 6: 537-544.

Lee, S., D. Choi, C. Park and S. Kim, 2009. An efficient key management scheme for secure SCADA communication. Int. J. Comput. Sci., 4: 180-180.

Ma, Z., P. Smith and F. Skopik, 2012. Towards a layered architectural view for security analysis in SCADA systems. Austrian Institute of Technology.

Majdalawieh, M., P.P. Francesco and D. Wijesekera, 2006. DNPSec: Distributed Network Protocol Version 3 (DNP3) Security Framework. In: Advances in Computer, Information and Systems Sciences and Engineering, Elleithy, K., T. Sobh and A. Mahmood (Eds.)., Springer, ISBN-10: 140205260X, pp: 227-234.

Manz, D.O., T.W. Edgar and G.A. Fink, 2010. A hybrid Authentication and authorization process for control system networks. Proceedings of the 6th International Conference on Information Assurance and Security, Aug. 23-25, IEEE Xplore Press, Atlanta, GA, pp: 36-39. DOI: 10.1109/ISIAS.2010.5604045

Moore, A.P., R.J. Ellison and R.C. Linger, 2001. Attack Modeling for Information Security and Survivability. 1st Edn., Carnegie Mellon University, Pittsburgh, pp: 21.

Musa, S., A. Shahzad and A. Aborujilah, 2013a. 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, Jan. 17-19, DOI: 10.1145/2448556.2448588

Musa, S., A. Shahzad and A. Aborujilah, 2013b. Simulation base implementation for placement of security services in real time environment. Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, (IMC ‘13), New York, DOI: 10.1145/2448556.2448587

NCSTIB, 2004. Supervisory Control and Data Acquisition (SCADA) Systems. National Communications System, Technical Information Bulletin.

NSTB, 2009. Enhancing control systems security in the energy sector. NSTB.

Patel, S.C. and J.H. Graham, 2006. Secure Internet-Based Communication Protocol for SCADA Networks. 1st Edn., University of Louisville, ISBN-10: 0542826542, pp: 195.

Patel, S.C. and Y. Yu, 2007. Analysis of SCADA security models. Int. Manage. Rev., 3: 68-76.

Patel, S.C., D.B. Ganesh and J.H. Graham, 2009. Improving the cyber security of SCADA communication networks. Commun. ACM., 52: 139-142. DOI: 10.1145/1538788.1538820

Rautmare, S., 2011. SCADA system security: Challenges and Recommendations. Proceedings of the Annual IEEE India Conference, Dec.16-18, IEEE Xplore Press, Hyderabad, pp: 1-4. DOI: 10.1109/INDCON.2011.6139567

RIPTECH Inc., 2001, Understanding SCADA system security vulnerabilities. RIPTECH Inc.

Robles, R.J. and M.K. Choi, 2009. Symmetric-key encryption for wireless internet SCADA. Proceedings of the International Conference, Sec Tech, Held as Part of the Future Generation Information Technology Conference, Dec. 10-12, Springer Berlin Heidelberg, Jeju Island, Korea, pp: 289-297. DOI: 10.1007/978-3-642-10847-1_36

Rush, W.F., J.A. Kinast, A.B. Shah, 2006. AGA 12 recommends how to protect SCADA communications from cyber attack. Pipeline Gas J., 233: 40-40.

Shahzad, S., A. Aborujilah and M. Irfan, 2014. A new cloud based supervisory control and data acquisition implementation to enhance the level of security using testbed.

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, 5: 19-24.

Singh, 2006. Intrusion detection in SCADA systems. J. Comput. Sci. Inf. Technol.

Stamp, J. and W. Young, 2003. Common vulnerabilities in critical infrastructure control systems. Proceedings of the Sandia National Laboratories Albuquerque, NM 87185- 0785, (SNL ‘03).

Stamp, J., W. Youn, J. William and J. DePoy, 2003. Common vulnerabilities in critical infrastructure control systems. Proceedings of the Sandia National Laboratories Albuquerque, NM 87185-0785, (SNL, 03).

Stouffer, J. and K. Kent, 2006. Guide to Supervisory Control and Data Acquisition (SCADA) and industrial control systems security. Proceedings of the of Standards and Technology Recommendations of the National Institute, (RNI ‘06), pp: 2-13.

Subasree, S. and N.K. Sakthivel, 2010. Design of a new security protocol using hybrid cryptography algorithms. IJRRAS.

Tuzzo, S., 2008. A plugn'play platform independent solution that eliminates unauthorized access without the use of passwords or encryption keys. Proceedings of the IEEE Conference on Technologies for Homeland Security, May 12-13, IEEE Xplore Press, Waltham, MA, pp: 79-85. DOI: 10.1109/THS.2008.4534427

UCI, 2012. Development of Security Standards for DNP. ICCP and IEC 61850, Copyright UCI.

Wang, C., F. Lan and D. Yiqi, 2010. A simulation environment for SCADA security analysis and assessment. Proceedings of the International Conference on Measuring Technology and Mechatronics Automation, Mar. 13-14, IEEE Xplore Press, Changsha City, pp: 342-347. DOI: 10.1109/ICMTMA.2010.603

West, A., 2008. Securing DNP3 and modbus with AGA12-2J. Proceedings of the 21st Century Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy, Jul. 20-24, IEEE Xplore Press, Pittsburgh, PA, pp: 1-4. DOI: 10.1109/PES.2008.4596340

Xiao, L., I.L. Yen and F. Bastani, 2010. Scalable Authentication and Key Management in SCADA. Proceedings of the International Conference on Parallel and Distributed Systems, Dec. 8-10, IEEE Xplore Press, Shanghai, pp: 172-179. DOI: 10.1109/ICPADS.2010.66

Zhu, B., A. Joseph and S. Sastry, 2011. A taxonomy of cyber attacks on SCADA systems. Proceedings of the International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, (PST ‘11), Washington, DC, USA, pp: 380-388. DOI: 10.1109/iThings/CPSCom.2011.34