Security Control Assessment of Supervisory Control and Data Acquisition for Power Utilities in Tanzania

Job Asheri Chaula, and Godfrey Weston Luwemba

***Abstract*—The primary purpose of this research was to assess the adequacy and effectiveness of security control of the Supervisory Control and Data Acquisition (SCADA) communication network used by infrastructure companies. Initially, the SCADA networks were physically separated from other networks connected to the internet and hence assumed secure. However, the modern SCADA are now integrated with other network resulting in new security vulnerabilities and attacks similar to those found in traditional IT. Thus, it is important to reassess the security controls of the SCADA because it is operated in an open network environment. In this research, a case of the SCADA security controls in the power sector in Tanzania was assessed, whereby a specific SCADA implementation was studied. The data were gathered using observation, testing, interviews, questionnaire and documentation reviews. The results were analyzed using the Cyber Security Evaluation Tool (CSET) and checked for compliance based on the National Institute of Standards and Technology (NIST) and North America Electric Reliability Corporation (NERC) standards. The findings have shown that there exist security vulnerabilities both in security compliance of the standard and component-based vulnerabilities. Additionally, there is inadequate of audit and accountability, personnel security and system and information integrity. Also, for the component-based security compliance, the finding shows that identification and authentication, security management and audit and accountability. On the basis of the results, the research has indicated the areas that require immediate action in order to protect the critical infrastructure.**

***Index Terms*—Supervisory Control Data Acquisition, Security Control, Network Systems.**

I. Introduction

Supervisory control and data acquisition (SCADA) systems are computer-based systems that find its applications many critical infrastructures and industries (e.g., electric grid, natural gas, water, telecommunications, and wastewater industries) to monitor and control sensitive processes and physical functions [1]. The SCADA communication networks allow operation of a number of devices located remotely; such as route switches, traffic signals, electric circuit breakers, valves, relays, sensors, and water and gas pumps [2]. Without a secure SCADA system, it is impossible to protect the nation's critical infrastructures. However, in the past, SCADA networks were separated from public networks by proprietary protocols and dedicated communication channels [3]. Consequently, the security of SCADA networks depended on the physical isolation from all other communication networks; hence attackers could not be able to access the SCADA system [4].

Published on July 13, 2020.

J. A. Chaula, and G. W. Luwemba,Computer Systems and Mathematics, Ardhi University, Dar es salaam, Tanzania.

It is now well established from a variety of studies, that the widespread interconnectivity of the SCADA system control network poses significant risks to the nation's critical infrastructures [5]. Without proper control of these computer systems and communication networks, individuals or organizations may disrupt the operations from remote locations for malicious purposes [6], [7]. When the SCADA network is connected to other computing networks, an unexpected threat that did not exist in the isolated SCADA system can occur at any in the network [8]. This makes the SCADA system also vulnerable to the usual or more common security attacks [9]. The architecture of the SCADA system comprises of one or more Master Terminal Units (MTUs) located at the central site used by operators to monitor and control a number of Remote Terminal Units (RTUs) installed in generation units or substations. The MTU is a computing platform on which SCADA management software is installed and RTUs or Intelligent Electronic Devices (IEDs) are normally small dedicated devices that are hardened for outdoor and industrial environments usage, [10]. The SCADA network is based on different communication channels and network technologies comprising Ethernet, serial links, and wireless communication.

II. Historical Attacks of SCADA Systems

The following examples illustrate both intentional and unintentional which happened in the past and caused the SCADA system's malfunctions [11] and [12]. These attacks occurred as a result of unauthorized persons gaining access to the critical infrastructures that operate SCADA systems.

i. In 1997, a teenager disconnected phone services at the control tower of Worcester Air Traffic Communications after he gained access to a computer system connected to Public Switched Telephone Network (PSTN) via dial-up connection. The attack also affected other sections, that is, airport security, fire department, weather services and aircraft carriers that use the airport. In addition to that, the tower's main radio transmitters and transmitter that activates runway lights were all shut down together with the printer used by controllers to monitor flight progress.

ii. In 2000, a disgruntled rejected employee at Maroochy Shire Sewage used radio transmitter remote access to the control system and released nearly 264,000 gallons of raw sewage to areas close to the station such as hotels, parks, and river.

iii. In 2003, the Slammer worm penetrated a computer network at the Davis-Besse Nuclear Power Plant

SCADA network and stopped the plant's safety monitoring system for about 5 hours in spite of plant operators' belief that the network is protected by a firewall. Also, the attack caused the plant's process computer to become unavailable for about 6 hours.

iv. In March 2008, plant shutdown occurred at the Hatch Nuclear Power Plant that was caused by software updates done on the plant's business network. The two networks were synchronized which enabled update done at the business network to synchronize with the SCADA network. The shutdown event caused no harm to the public, but the power plant lost millions of dollars in revenue to restore the plant back.

v. In July 2010, the Windows computer worm, Stuxnet, was propagated in the industrial software and equipment. The worm was targeted only to Siemens SCADA with a highly specific payload to reprogram the operation of the attached uranium-refining centrifuges in the Iranian facilities [13].

Tanzania is one of the developing countries and having infrastructure utilities of the above natures is not isolated from the occurrence of the above calamities if the SCADA communication network is not secured. In consideration of the sensitivity of the information to be collected, analyzed and ultimately presented in the final report, there is a need for some level of confidentiality to be provided; especially for the organization that has been used as a case study. Therefore, the purpose of this research was to assess the adequacy and effectiveness security control of the context-specific implementation of the SCADA communication network.

III. Methodology

A case study approach was adopted to assess the security control of the implemented SCADA communication network. In carrying out the security control assessment the North American Electricity Reliability Corporation (NERC) standard was selected to assess the security control as it covers all the important areas of the SCADA network. The SCADA security control assessment was performed to determine the extent to which the security controls for the SCADA network at the case study satisfy the requirements of NERC CIP, Minimum Security Requirements for critical electric grid infrastructures. In addition to the NERC standard, the NIST SP 500-53A standard "Guide for Assessing the Security Controls in Federal Information Systems" procedures were used to evaluate the effectiveness of the security controls of the implemented at SCADA communication network at the case study.

The security control assessment process involved three methods that are, observe, interview and test. These methods were used to determine the security controls that are implemented in the case study to secure SCADA critical cyber assets. In the first method, the evidence was collected through observing, checking, studying and inspecting an object relating to the security control under assessment. The second method was all about conducting a discussion with personnel involved in the operation and administration of the SCADA system. The third method involved performing actions to one or more assessment objects and in this case, the actions were performed to non-critical cyber assets to avoid causing malfunction to the system under operation. These non-critical cyber assets included systems that help to provide security to critical assets (NIST SP800-53A). Table I gives a description of the assessment methodology used in this study to assess the adequacy and effectiveness of the implemented security controls. The analysis of the collected data was further analyzed by the Cyber Security Evaluation Tool (CSET).

TABLE I: Description of Security Controls Assessment Methodology

Assessment Method	Assessment Object	Object Components
Examine	Specifications	Security policies, Security plans, Security procedures, SCADA system requirements, SCADA system design
	Mechanisms	The functionality implemented in SCADA hardware and Software
	Actions	SCADA system operations, Administration
Interview	SCADA personnel (Individuals or group of individuals)	SCADA senior manager and engineers
Test	Mechanisms	The functionality implemented in SCADA hardware and Software
	Actions	SCADA system operations, Administration

A. Establishing the Baseline Security Controls Requirements

The technical security controls were assessed based on the NERC CIP standards and requirements as shown in Table II. The assessed security control was evaluated against this requirement to determine the adequacy and effectiveness of the control in place. If any information is different from the standard it signifies that the security control is not adequate.

TABLE II: NERC CIP Standard and Requirements

NERC CIP Security Requirements
Security Management Controls
R1.2- "The cyber security policy is readily available to all personnel who have access to or are responsible for Critical Cyber Assets"
R5- "Implement a program for managing access to protected Critical Cyber Asset information"
R5.2- "Review at least annually the access privileges to the protected information to confirm that access privileges are correct"
Electronic Security Perimeter Controls
R2.1- "Use an access control model that denies access by default"
R2.2- "Enable only ports and services required for operations and for monitoring Cyber Assets within Electronic Security Perimeter"
R2.3- "Implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter"
R2.4- "Implement technical controls at the access points to ensure the authenticity of the accessing party"
R3.2- "Detect and alert for attempts at or actual unauthorized accesses"
R4.2- "Review to verify that only ports and services required for operations at these access points are enabled"
Physical Security Controls
R1.2- "Identification of all physical access points through each physical security perimeter and measures to control entry at those access points"
R2.1- "Protect Physical Access Control Systems from unauthorized physical access"
R3- "Protect Electronic Access Control Systems from unauthorized electronic access"
R4- "Implement physical access controls to manage physical access to all access points to the Physical Security Perimeter 24-hour a day, 7 days a week"
R5- "Implement the technical and procedural controls for monitoring

physical access at all access points to the PSP"
R6- "Implement and document procedural mechanisms for logging physical entry at all access points to the PSP"
Security Systems Management
R1.1-"Create, implement and maintain cyber security test procedures"
R2- "Implement a process to ensure that only those ports and services required for normal emergency operations are enabled"
R3.1- "Assessment of security patches and security upgrades for applicability within thirty calendar days of availability"
R4.2- "Implement a process for the upgrade of anti-virus and malware protection signatures"
R5 – "Establish, implement and document technical and procedural controls that enforce authentication of and accountability for all user activities"
R5.1.3-"Review at least annually user accounts to verify access privileges"
R5.3-"Require and user passwords subject to the following", "six characters" "combination of alpha, numeric and special characters and changed at least annually"
R6.3-"Maintain logs of system events related to cyber security"

B. *The Identification of Critical Cyber Assets*

To perform security controls assessment of the SCADA communication network implemented at the case study we used the risk-based methodology to identify critical cyber assets. The identification process in this research focused on electronic devices that can be configurable or programmed to meet an intended functionality as one of the criteria to qualify the device to be a critical cyber asset such as routers, switches, workstation, network firewall, intelligent electronic devices, etc. Fig. 1 shows the decision flow chart for critical cyber asset identification.

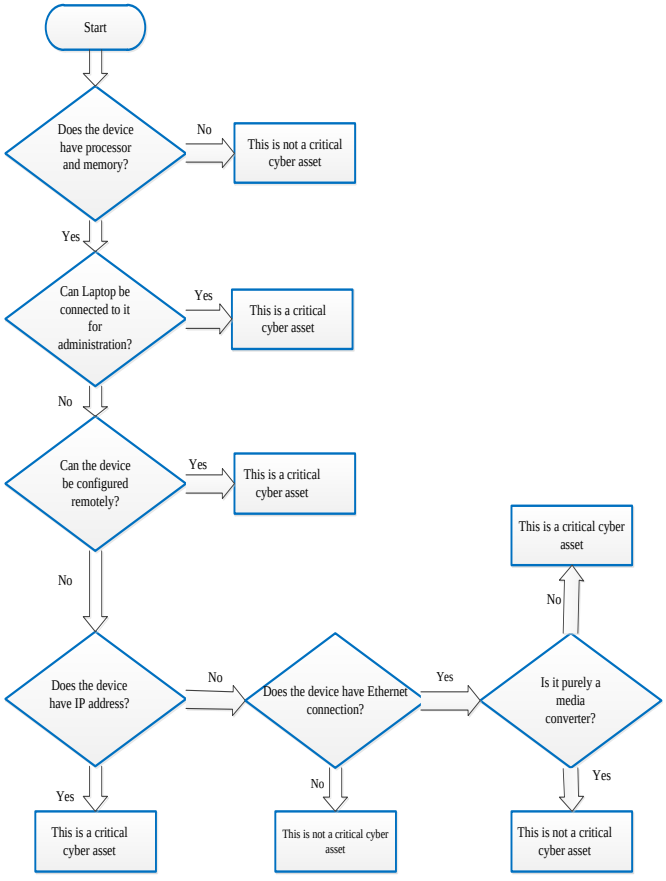

Fig. 1. Flow chart for identifying device's critical asset status

C. *Analysis of SCADA Component Security Compliance using CSET*

This particular case analyses the component or devices connecting up the SCADA communication network. The results were the response to questions generated from the network diagram which represents the network implemented at the case study. Table III shows the general component compliance for each device making up the SCADA communication network and the combined percentage at which the component meets the security assurance level (SAL). For example, the questions meeting the targeted security assurance level for VPN is 100% whereas for the Database server the questions meeting targeted SAL is only 4%. The largest gap in the database server is due to the use of simple passwords using a challenge-response protocol for authentication. The general component security compliance is shown in Table III.

TABLE III: COMPONENT COMPLIANCE SUMMARY USING CSET

Component	Percent of Questions Meeting Target SAL	Percent of Questions 1 SAL below Target SAL	Percent of Questions 2 SAL below Target SAL	Percent of Questions 3 SAL below Target SAL	Percent of Questions 4 SAL below Target SAL
VPN	100%	0%	0%	0%	0%
Modem	69%	31%	0%	0%	0%
Router	58%	6%	7%	29%	0%
RTU	44%	27%	3%	26%	0%
HMI	42%	8%	12%	38%	0%
Switch	33%	5%	19%	43%	0%
FEP	29%	6%	29%	36%	0%
Firewall	25%	13%	19%	43%	0%
Application Server	11%	24%	5%	60%	0%
Database Server	4%	28%	10%	19%	39%

For database server and application servers, the largest gap in compliance is related to lack of audit and accountability and the system not configured to alert the administrators in the event of a security violation

IV. RESULTS AND DISCUSSION

A. *SCADA Component Security Compliance as per NERC Standard*

The component security compliance in Fig. 2 resulted from the configuration done on an individual component that connects the SCADA network. Ranking the subjects was based on the security attributes configured for each individual component.

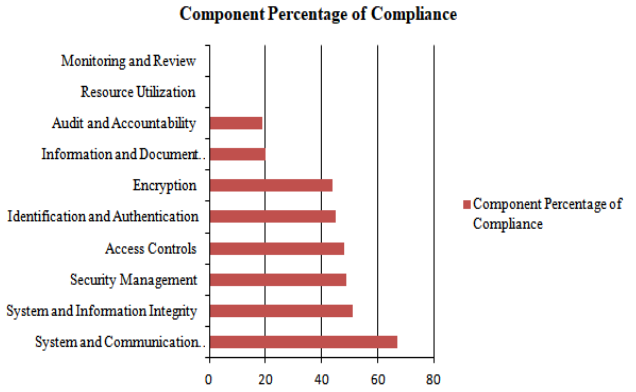

Fig. 2. Component security compliance to the standard

From the data in Fig. 2, it is apparent that system and communication protection with 67% have higher SCADA component security compliance while audit and accountability represent high risks with 19%. This indicated the lack of audit and accountability to the SCADA system which could result in the system being compromised.

B. NERC Standard Security Compliance

From the network analysis performed, the NERC compliance was evaluated after responses to the questions as aggregated from observation, interviews and questionnaire results. The results indicated the percentage of standard security compliance out of 100% evaluated based on the subject area. For example, security management indicates it complied 45% which implies that the responsible organization should review the subject area to increase the compliance level and protect the critical system from being compromised by attackers.

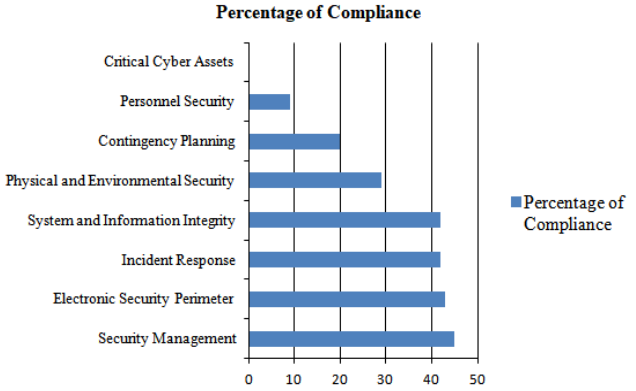

Fig. 3. The NERC standard compliance by subject area

In Fig. 3, the security standard compliance for all the subject areas is below 50% which implies that security risks are high in the context. This means that the organization needs to work more on the remaining percentage to fix the weaknesses that could allow an attacker to gain access to the SCADA system.

C. NERC Standard Security Compliance Ranked by Subject Area

A check against the NERC standards implementation in the context was performed for security compliance. In Fig. 4, shows the NERC standard security compliance ranked by subject area in which the percentage of each subject indicates the contribution in terms of security deficiencies for the particular subject area. This means that the weakness that was found, for example on the system and information integrity have a high risk for the system to be compromised by attackers.

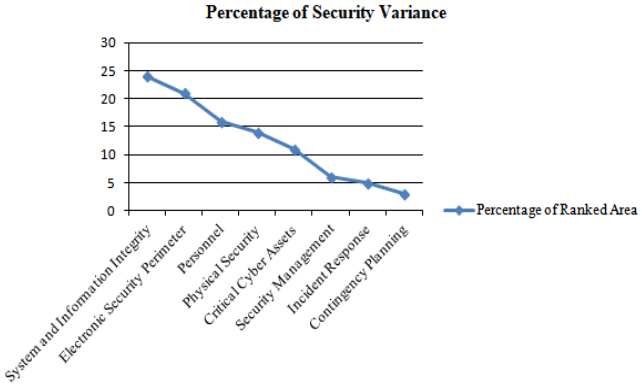

Fig. 4. NERC compliance ranked by subject area

Fig. 4 exhibits the subject area that needs more attention in the order of importance from the security point of view. According to the graph, the prominent five areas that need to be addressed by the organization to comply to NERC are System and information integrity, electronic security perimeter, personnel, physical security, and critical cyber assets. For instance, the percentage contribution of system and information integrity should be addressed by disabling all ports and services that are not needed, security patches and antivirus upgrades, review of user accounts to verify access privileges and implement technical and procedural mechanisms for monitoring security events on all cyber assets within the perimeter. By addressing the security concerns for the first five subject areas means that the percentage of compliance will be balanced to an acceptable level above 50%.

D. SCADA Component Security Compliance Ranked by Subject Area

The result is a combined effect from all the components connecting the SCADA network as analyzed from the power utility. The finding from Fig. 5, shows the subject area contribution in terms of percentage security variance aggregated from different components making up SCADA network indicated areas that the organization should pay attention in order to enhance security either from the configuration point of view or system administration. The higher the percentage of security variance indicates the area that the power utility should address in order to protect the system.

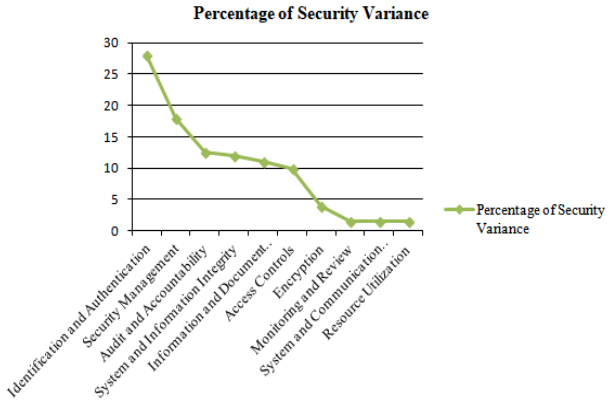

Fig. 5. Component compliance ranked by subject area

The graph in Fig. 5, shows the security control areas that require serious attention to protect the system from being compromised. It represents a total weighted value of 100% of the security variances identified in each ranked subject area. Based on the component analysis, it was found that more attention is needed to alleviate discrepancies resulting from the identification and authentication of users and devices to the critical cyber assets. Apart from identification and authentication, other areas that require serious attention include security management, audit and accountability, system and information integrity.

V. Conclusion and Recommendation

A. Conclusion

The present study was designed to assess the adequacy and effectiveness of security control SCADA specific implementation as a measure to enhance the security posture of the SCADA system. The security control was assessed based on the controls implemented under North American Electricity Reliability Corporation (NERC) standards which cover wholly the parts of securing SCADA network for power utilities. The security controls of the implemented SCADA network were assessed and found that there exists no SCADA specific security policy, inadequate password management, and handling, inadequate authentication mechanisms and lack of network segmentation. As per the briefing of the findings above, it is obvious that the implemented security controls of the SCADA communication network used by context are not adequate and effective to address all the vulnerabilities that could occur as a result of identified weaknesses. The exploitation of any of the above weaknesses by an unauthorized person to the critical assets that facilitate SCADA system functionality could result in loss of life, equipment damage and affect the economy of the country. The result of this research indicates that securing the SCADA communication network used by utility companies in order to protect access to data from unauthorized attackers.

B. Recommendation

The security control assessment of the SCADA communication network requires significant attention and resources due to SCADA operation constraints. Security assessment tools cannot be used directly in the production system as it might cause the system to malfunction or damage the critical cyber assets. In this work, the focus was to assess the security control of the SCADA communication network. Further research can be done by implementing SCADA testbed comprising all components making up the SCADA system where security can be tested before deploying to the production system.

Acknowledgment

The authors wish to thank the world bank for their valuable financial support to this work.

References

[1] Y. Wang, "sSCADA: securing SCADA infrastructure communications," *Int. J. Commun. Networks Distrib. Syst.*, vol. 6, no. 1, pp. 1–13, 2010.

[2] H. G. Sandip, C. P., Ganesh, D. B., and James, "Improving Cyber Security of SCADA Communication Networks," *Commun. ACM*, vol. Vol. 52, no. No. 7, p. pp 139-142, 2009.

[3] T. Adams, "SCADA Systems Intermediate Overview," in *Technical Information Bulletin 04-1*, 2004, no. 877, pp. 1–64.

[4] Z. Jianqing, "Secure Multicast for Power Grid Communications," PHD Thesis, University of Illinois at Urbana-Champaign, 2010.

[5] A. Cook, H. Janicke, L. Maglaras, and R. Smith, "An assessment of the application of IT security mechanisms to industrial control systems," *Int. J. Internet Technol. Secur. Trans.*, vol. 7, no. 2, pp. 144–174, 2017.

[6] C. Ten, C. Liu, and M. Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees," in *IEEE Power Engineering Society General Meeting*, 2007, no. July.

[7] L. Yang, X. Cao, and J. Li, "A new cyber security risk evaluation method for oil and gas SCADA based on factor state space," *Chaos, Solitons and Fractals*, vol. 89, pp. 203–209, 2016.

[8] A. Hristova, R. Schlegel, and S. Obermeier, "Security assessment methodology for industrial control system products," *4th Annu. IEEE Int. Conf. Cyber Technol. Autom. Control Intell. Syst. IEEE-CYBER 2014*, pp. 264–269, 2014.

[9] S. Araghi and A. A. Shams-baboli, "Improving Security in SCADA Systems," 2012.

[10] J. H. Graham and S. C. Patel, "Security Considerations in SCADA Communication Protocols," *Comput. Eng.*, no. 502, pp. 1–24, 2004.

[11] R. Tsang, "Cyberthreats, vulnerabilities and attacks on SCADA networks," *Univ. California, Berkeley, Work. Pap. …*, pp. 1–23, 2010.

[12] Z. Cheah and A. B. M. O. Faruk, "Identifying and Responding to External Threats in a PCS Network," Norwegian University of Science and Technology, 2007.

[13] S. Venkatraman, "Cybersecurity in Power Systems," MSc Thesis, Georgia Institute of Technology, 2012.

Dr. Chaula Job Asheri was born in Mufindi Iringa Region on 12.4.1968. He holds a Bachelor's of Science in Physics and Electronics of the University of Dar es Salaam, Dar es Salaam Tanzania, 1996, Masters of Science in Computer and Systems Sciences of the University of Stockholm, Stockholm Sweden, 2003 and PhD in Computer and Systems Sciences of Stockholm University, Stockholm Sweden, 2006. His major field of study is computer and Systems security.

He is currently employed as a SENIOR LECTURER in computer and Systems Sciences at Ardhi University, Dar es Salaam, Tanzania. Previous research interests include ICT for Development, computer systems security and the current research interests include remote sensing, Geographic information systems, spatial data science and internet of things.

Dr. Chaula is a member of the Tanzania Commission of ICT. He has made significant contribution to the Tanzania Commission of Higher Education, Namibia Council for Higher Education, Kenya and Uganda Commission for Higher Education and Inter University Council for East Africa curriculum review for accreditation and Universities institutional audits in Uganda, Tanzania, Namibia and Kenya.

Godfrey Luwemba received BSc and MSc in telecommunications engineering from University of Dar es Salaam, Tanzania, in 2008 and 2015 respectively. He is currently working toward PhD degree.

Since 2010, he has been with Ardhi University, Tanzania, as an academic member of staff in the department of Computer Systems and Mathematics. His interests include channel modeling, physical layer security for both WiFi and powerline communications. He also works on smart grid communications.

Mr. Luwemba is a member of professional bodies including Engineers Registration Board, Tanzania, and Association of Computing Machinery (ACM), USA.