An Ontology of Cyber Security Automation

Mrityunjay Brahma[1], Hemanta Kumar Kalita[2]
Central Institute of Technology, Kokrajhar
Corresponding author: Hemanta Kumar Kalita, Email: hkkalita@cit.ac.in

Automation has been a major challenge for many industries (from small to large scale) in the fight against rising cyber threats. Many tools and techniques has been developed to fight against the rising security threats. Cyber criminals carry out a broad range of cyber attacks with various tactics and tactics against organizations and individuals in order to compromise and breach organization's network, data and the three aspects of it i.e Confidentiality, Integrity and Availability. Nowadays, organizations need a specific plan that focuses on cyber security retention. The Corona Virus Disease-2019 pandemic has created new challenges for businesses as they adapt to an operating model in which working from home has become the 'new normal'. Companies are accelerating their digital transformation and the cyber security aspect is an important and a major upkeep challenge.

Keywords: Cyber Security, Security Automation, Automation

2023. In Satyasai Jagannath Nanda & Rajendra Prasad Yadav (eds.), *Data Science and Intelligent Computing Techniques*, 135–147. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.56155/978-81-955020-2-8-12

1. Introduction

In recent years, networks have evolved from a mere means of communication to ubiquitous computer infrastructure. Networks have become bigger, faster, and more flexible. Computers are everywhere. Almost all of us in our daily lives depends on computers and computers net-works. The internet has technically become a very important tool and a medium for governments, corporations, and financial institutions to carry out their day to day business digitally. In early days most people didn't use them as a primary source of communication and information. But with time computers and networks are used for control and managing production processes [5], water supply, power grid, air traffic control systems, and stock market plans, to name a few. The exponential growth of the Internet interconnections has led to a significant growth of cyber attack incidents often with disastrous and grievous consequences. Cyber crooks are now casting a wider net, attacking not just PCs and mobile phones but also Internet-connected devices like security cameras or routers, which has "exponentially" increased the risk landscape. Therefore, cyber security has become foremost part of cyber world because it encompasses everything that relates to protecting our data from cyber attackers who want to steal information and use it to cause harm. In the context of cyber security there are plethora of jobs where some can be automated and some can't. Also there are plenty available training programs, most of which are paid, however there are several where participation is free. Cyber security is a comprehensive area that is inclusive of software features, hardware, human resources, functional processes, as well as mental functioning. The same is for the range of security threats, which can be in varied ways and forms that can cause damage at different levels and with different severity. Therefore, awareness and training is an effective way to deal with online security threat.

Cyber security is an application that protects computer systems and networks from unauthorized access, theft, or damage to hardware, software, or data [8], [18]. The purpose is to take security measures to protect critical infrastructure and sensitive information from malicious individuals. Cyber security (aka IT security) measures, are designed to combat threats to networked systems and applications, whether they originate from inside or outside the organization [1]. Anyone involved in technology can be a victim of cybercrime.

Agencies have a variety of cyber security solutions to choose from. These cyber security solutions help agencies protect their data at different stages of their lives. That includes when data is first collected, time when it is transmitted between different systems and users and between storage until it is deleted. Although there are many different systems at various levels for various functions, they all have the same purpose: To provide institutional visibility to what is happening on their computer networks and to warn the technical leaders of any anomilies.

In this paper we have done a survey on different jobs related to cyber security personnel as well as whether it can be automated or not. The remainder of this paper is organized as follows. In the following section i.e section 2, we surveyed different existing literature. Then in section 3, we classified different cyber security automation tasks. After that this paper ends with conclusion and references.

2. Literature Review

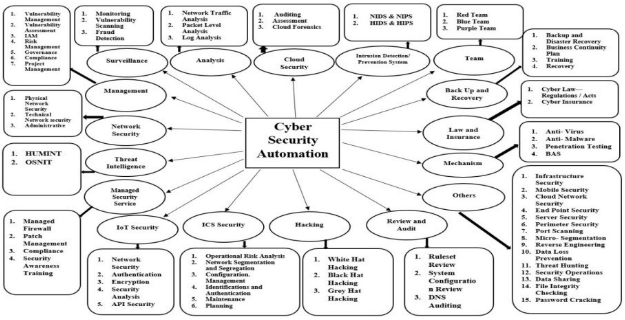

Fig. 1: Cyber Security Automation Operations

Author R. A. Kemmerer in Paper [1], introduces some well-known threats to cyber security, threat detections and analyzes security measures and threats to combat threats. Ways to prevent, detect, and response to cyber-attacks are also been discussed here.

Authors M. Evans et al. in paper [2], discussed about the understanding typical behaviour of human is vital to identifying anomalies and preventing cyber attacks. Beside this authors proposed a high-level cyber security human vulnerability model for quantifying range of human aspect tasks that provide, or are intended not to negatively affect cyber security posture.

Authors F. Alotaibi et al., in Paper [3] and F. Alkhudhayr et al., [4], gave few tools and techniques that would increase the security related to one of the four fields (information system, cyber space, IoT and network). Moreover from paper [3] we have learned that the best ways of combating cybercrime is by creating awareness among the people and adopting better cyber security practices and maintain cyber hygiene.

Author P. Kampanakis in [18], mainly discussed about the available security information-sharing options and the risks associated with it during information exchange.

Authors S.M. Mohammad and S. Lakshmisri in Paper [6], has discussed about the dependencies and the support of security automation. Author has also enlisted some security automation tools based on the need of industries.

T. AlSadhan and J.S. Park in paper [7] discussed the principles of and requirements for Information Security Continuous Monitoring (ISCM) and Risk Manangement in support of cyber defenses, real-world challenges.

3. An ontology of cyber security automation

Cyber security is essential about protection of company hardware, software, and networks from cybercriminals. Cyber Security professionals are responsible for providing security for an organization's overall IT systems. They monitor and look for search for vulnerabilities in software, hardware, networks and design strategies and defensive systems to protect against attacks and threats. Enlisted in Fig.1 various tasks related to cyber security automation which are inside the oval shapes and after that we sub-categorized those tasks which are inside the rounded rectangle shapes. A particular cyber security task prepares for and responds to cyber attacks. These tasks in might be meant for different purposes, but the general idea remains the same.

3.1 Analysis

Analysing is a process of reviewing all the factors that come with a particular asset or event. Analysis is a proactive approach to cyber security that uses data collection, aggregation capabilities to perform vital security functions on network traffic, packet level traffic inspection and also analysing of different event logs [16] generated from different log sources.

Network Traffic Analysis- Network traffic analysis is a process of checking all the incoming and outgoing traffic and its metadata and contexts to determine any kind of threats. Automation is possible.
Packet Level Analysis- Packet level analysis is a forensics technique to check the details of the packet i.e the data from where it has been coming and to which system or network is going and also helps in determining if a networked device is infected with malware or not. It is possible to automate these operations.
Log Analysis- Computers, networks, and other IT systems generate records called audit trail records or logs that document system activities. Log analysis is the evaluation of these records and is used by organizations to help mitigate a variety of risks and meet compliance regulations. It is possible to automate these operations.

3.2. Backup and Recovery

These are the processes which helps in getting back to normal operation after any disaster or unexpected outrage period. It includes disasted recovery [2], business continuation plan and training [11] .

Backup and Disaster Recovery- Back is a process of making extra or multiple copies of data.
Whereas disaster recovery is a step-by-step process of planning on how to recover after an outrage.
Automation is possible

Business Continuity Plan- Business continuity planning helps in ensuring that the proper pro-cesses are being put in place and resources are allocated to help in a smooth transition as they recover from a cyber-attack. Automation is not possible as different business is of different type and to run it one has to make a different plan from others.
Training- It is process of sharing the knowledge of system, networks and the working of things in cyber world with others working under the same environment. It is not possible. **Recovery**- Recovery is essentially a process of restoring back to normal state after an outrage.
Automation is possible.

3.3. Cloud Security

Cloud security, also known as cloud computing security, is a collection of security measures such as auditing, assessment and cloud forensics [4], [8], [9] which are design to protect cloud-based infrastructure, applications, and data. These measures ensure user and device authentication, data and resource access control, prevent fraud and provide data privacy protection.

Auditing- Audit is a systematic and independent examination of an organization's cyber se-curity. An audit ensures that the proper security controls, policies, and procedures are in place and working effectively. Automation is possible.
Assessment- Assessment is a process of evaluating security controls to examine the overall organization's security infrastructure. Automation is possible.
Cloud Forensics- Cloud forensics refers to investigations that are focused on crimes that occur primarily involving the cloud. This could include data breaches or identity thefts. Automation is possible.

3.4. Hacking

Hacking is a process of gaining access to a system or network through some unwanted authentication or authorization or method. It includes white hat, black hat and grey hat hacking.

White Hat Hacking (uncover security loopholes)- White hat hacking is one kind of ethical hacking where professional who uses their skills to identify vulnerabilities in software, hardware, and networks. Automation is not possible.
Black Hat Hacking (exploits vulnerability)- Black hat hacking is the practice of exploiting vulnerabilities of a system or network with malicious intent. Automation is not possible.
Grey Hat Hacking- Grey hat hacking is a combination of white hat and black hat categories. In Gray hat hacking one may exploit vulnerabilities for personal gain, but they also occasionally disclose these vulnerabilities to the affected parties or the general public. Automation is not possible.

3.5. ICS Security

Industrial Control System (ICS) [15] is one of the different types of control systems that are used for different purposes like operational risk analysis, network segmentation and segregation [11], [15], planning and many more in the industrial processes. It can be composed of just a few controllers or a complex network of interactive control systems made up by hundreds or thousands of connections.

Operational Risk Analysis- Operational risk analysis is reviewing the risks related to a spe-cific operation or actions. Automation is not possible.
Network Segmentation and Segregation- Network segmentation involves partitioning a network into smaller networks; while network segregation involves developing and enforcing a ruleset for controlling the communications between specific hosts and services. Automation may be or may not be possible as how a large network can be segmented and what are the rules must be enforce on it.
Configuration Management- Configuration management is a process for maintaining computer systems, servers, and software in a desired, consistent state. Here also automation may be or may not be possible as different system or network has different configuration.

Identification and Authentication- Identification is the ability to identify uniquely an user of a system or an application that is running in the system. Authentication is the ability to prove that an user or application is legit and who they claims to be. Automation is possible.
Maintenance- Maintenance is a practice of keeping things on regular form. Automation is possible. **Planning**- Planning is an organisation's written strategies to follow and improve its overall risk management and defences against the on-going threat of cybercrime. Automation is not possible.

3.6. Intrusion Detection/ Prevention System

Intrusion detection and prevention systems are the primary defence system to a network or system which detect any unwanted behaviour in the incoming or outgoing traffic and prevent it from causing any harm to th e organization's system or network. Technically, it has four different functions: Network Intrusion Detection System (NIDS), Host Intrusion Detection System System (HIDS), Network Intrusion Prevention System (NIPS) and Host Intrusion Prevention System (HIPS) [9] - [11].

Network Intrusion Detection and Prevention System (NIDS & NIPS)- Detects and prevents (blocks) intrusion across your entire network, using all packet metadata and contents to determine threats. Automation is possible.
Host-Based Intrusion Detection and Prevention System (HIDS & HIPS)- Detects and prevents (blocks) intrusion through a particular endpoint and monitors network traffic and system logs toand from a particular device. Automation is possible.

3.7. IoT Security

Security in IoT is the act of securing Internet devices and the networks by authenticating, encrypt-ing, analysing [12], [13] from threats and breaches. It also includes network security and API security.

Network Security- Network security is a process of defending the networking infrastructure from any unauthorized access, misuse, or theft. It involves creating a secure infrastructure for devices, applications, users, and applications to work in a secure manner. Automation is possible.

Authentication- Authentication is a process of proving or verifying the identity of a person or device. Automation is possible.
Encryption- Encryption is the method by which information is converted into secret code that hides the information's true meaning. Automation is possible.
Security Analytics- Security Analytics is an approach to cybersecurity focused on the analysis of data to produce proactive security measures. Automation is possible.
API Security- API security is the protection of the integrity of APIs (Application Programming Interface). Automation is possible.

3.8. Law and Insurance

Consumers and businesses rely heavily on technology to interact with each other. As technology is everchanging, so are the rules governing the use of the data that is being collected. Laws [14], help an organization or individiual to protect its identity that is shared over internet. Insurance [16] guaranted that any Loss added by Extension is covered only to the extent.

Cyber Law— Regulations / Acts- Cyber law or internet law is a part of overall legal system of that is related to internet or cyber world. It provides the legal right and protection to the individuals, Intelectual Properties using the internet. Automation is not possible.
Cyber Insurance- Cyber insurance is an insurance product designed to help businesses against the potentially devastating effects of cybercrimes. Automation is not possible.

3.9. Managed Security Services

It is an outsourcing process and management of different security services. This is a multi-tenant environment providing common security services such as log aggregation, event monitoring, analysing and reporting, firewall, patch management, compliance and security awarness training [4] - [6].

Managed Firewall- Firewall is a barrier that checks and filter all the inbound and outbound traffic so that no unwanted traffic can enter or leave the perimeter of an organization. These process can be automated.
Patch Management- Patch management is the process of fixing software bugs by applying updates, which helps keep your systems up and running. These process can be automated.

Compliance- Rules and Regulations that an organization put as an action of complying. These process can be automated.
Security Awareness Training- Security awareness training is essentially an educational program and strategy that helps the IT and security professionals to prevent and mitigate user risk. These programs are designed to help users and employees understand the role they play in helping to combat information security breaches. These process can't be automated as there are different types of training regarding security awareness.

3.10. Management

Management [8] is an organisation's strategic-level capability that control or organise all the events related to it. The goal of security management procedures is to provide a foundation for an organization's cybersecurity strategy like governance, compliance [10], project management, IAM, vulnerability assessment [6], [8].

Vulnerability Management- Vulnerability management is generally defined as the process of identifying, categorizing, prioritizing, and resolving vulnerabilities across endpoints, workloads, and systems. It is not possible to automate these operations.
Vulnerability Assessment- Reviewing systematically i.e. identifying, classifying and prioritizing all the weakness of system(s) or networks(s). It is possible to automate these operation.

Identity and Access Management (IAM)- IAM is a security discipline which gives privilege to all authenticate users or entities/ system to use the right resources (applications or data) when they need to, without interference, using the devices they want to use. It is possible to automate these operation.
Risk Management- It is a non-stop process of identifying, evaluating and addressing an organiza-tion's cyber security threat. It is possible to automate these operation.
Governance- It relates to the strategies used by an organization to fight against cybercrime and protects its IT infrastructure. It is possible to automate these operation.
Compliance- Rules and Regulations that an organization put as an action of complying. It is possible to automate these operation.
Project Management- These are the activities that are designed to reduce risk and help the organization to grow. It is not possible to automate these operation as many projects are there and every project is of different type from its previous one.

3.11. Mechanism

Under this, various tools comes which helps in fighting against any unwanted activities which can occur in due course of time. Common tools in cyber security are Security Incident and Event Management (SIEM), anti-virus, anti-malware [7], [14] .

Anti-Virus- Anti-virus is a type of software that is designed to protect your system against any type of virus that are designed to harm your system. Automation is possible. **Anti-Malware**- Anti-malware is a software tools and programs designed to identify and prevent malicious program from any infected system. Automation is possible.

Penetration Testing- Also known as "pen testing" is a simulation to a cyber-attack to know all the system vulnerabilities that can be exploits. It helps organizations manage risk, protect clients from data breaches, and increase business continuity. Automation is possible.

Breach and Attack Simulation (BAS)- BAS offers continues testing and validation of security controls and it test the security posture against any external or internal threats. Automation is possible.

3.12. Network Security

It is a set of rules and configurations designed to protect the confidentiality, integrity and acces-sibility of computer networks and data using both software and hardware technologies. Under network security, physical, technical and administrative network security [8] comes all together.

Physical Network Security- Physical security controls are designed to prevent unauthorized personnel from gaining physical access to network components such as routers, cabling cupboards and so on. Controlled access, such as passwords, biometric authentication is essential in any organization. Automation is possible if we segment the entire network and every segment has different responsibility.
Technical Network Security- It protects data and systems from unauthorized personnel, and it also

needs to protect against malicious activities from employees. Automation is possible. **Administrative Network Security**- Administrative security controls consist of security policies and processes that control user behaviour, including how users are authenticated, their level of access and also how IT staff members implement changes to the infrastructure. It may be or may be not possible to automate as administrative has a huge responsibility and sometimes it has to be done manually to overcome some process.

3.13. Review and Audit

The process of examining or considering again of something in order to decide if changes are necessary. It includes rule-set review, system configuration review [15] - [18].

Ruleset Review Practice of looking for security configuration issues, vulnerabilities and un-necessary rules that could lead to a breach in a network. Automation is not possible as there are different rules.
System Configuration Review- Configuration review is a detailed review and verification of configuration settings of IT infrastructure components including systems, network devices & applications to measure the security effectiveness of the IT environment. Automation is possible. **DNS Auditing**- DNS auditing is process of checking your DNS records. Automation is possible.

3.14. Surveillance

It is the practice of watching something or somebody to make ensure that everything is running smoothly and according to pre-define path. In terms of cyber security supervising is monitoring, vulnerability scanning and detecting [5], [6] any unwanted activities in a system(s) or network(s).

Monitoring-Keeping eye on all the operations of systems or networks and collecting data on regularly basis that measures progress towards achieving the goal. It is possible to automate monitoring
Vulnerability Scanning- It is a process of detecting and then classifying all the possible potential exploitation points presents in systems, networks and applications. Vulnerability scanning can be done automatically
Fraud Detection- It is a process to detect scams and prevents fraudsters from obtaining money or property (information) by illegal means. Automation is possible in this process
Detection- It is a process of analysing system(s) and network(s) of an organization to identify any malicious activity or vulnerability present within the organization. Automation is possible.

3.15. Team

Teaming is a group of professional individuals that collectively works towards a common goal. From a security testing perspective they together simulate a real life attack to help measure how well an organization can withstand the cyber threats and malicious actors of today. Red teaming, Blue teaming and Purple teaming are all part of it.

Red Team (offensive)- Red teaming is the practice of asking a trusted group called (ethical hackers) of individuals to launch an attack on your software or your organization so that you can test how your defences will hold up in a real-world situation. These red teams play the role of attackers by identifying security vulnerabilities and launching attacks within a controlled environment. Automation is not possible.
Blue Team (defensive)- Blue teams evaluate organizational security environments and defend these environments from red teams. Automation is not possible.
Purple Team- Purple teaming is a security methodology in which red and blue teams work closely together to maximise cyber capabilities through continuous feedback and knowledge transfer. Automation is not possible.

3.16. Threat Intelligence

Threat Intelligence is the knowledge of all threat which had occured or can occur due to some vulnerabilities in a system or network. Most common threat intelligence are HUMINT and OSNIT [9], [18].

Human Intelligence (HUMINT)- HUMINT is a process of collecting and evaluating data through inter-personnel (person to person) contacts and putting all the pieces together to get a bigger picture of the event. It is not possible to automate these operation as many information can be gathered from a human.
Open Source Intelligence (OSNIT)- OSINT refers to all information that can be found publicly this include both online and offline resources without breaching any copyright or privacy laws. This process can be automated.

3.17. Others

Infrastructure Security- Infrastructure security [14] is the practice of protecting all the system and assets against any cyber threat. Automation is possible.
Mobile Security- Mobile security [3] also called wireless security, which refers to the protection of mobile devices against cybersecurity threats. Automation is possible.
Cloud Network Security Cloud network security [3] is an area of cybersecurity focused on minimizing the chances that malicious actors can access, change, or destroy information on a public or private cloud network. Automation is possible.
End Point Security- End point security [12] is a process of defending all the devices or ports that are susceptible to any cyber attack. Automation is possible.
Server Security- Server security [12] is the process of securing the server of an organization from an attack. Automation is possible.
Perimeter Security- Perimeter security [15] refers to the process of defending a company's network boundaries from hackers, intruders, and other unknown individuals. Automation is possible. **Port Scanning** - Port scanning [15] is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities. Automation is possible. **Micro-Segmentation** [15]**-** It is a process of dividing large network into small distinct segments down to the individual workload level. Automation is possible.

Reverse Engineering- It is a process or method through which one attempts to understand through deductive reasoning how a previously made device, process, system, or piece of software accomplishes a task with very little (if any) insight into exactly how it does so. Automation is possible.

Data Loss Prevention- Data loss prevention is the function of protecting sensitive data from getting lost or stolen from any kind of security breaches. Data loss leads to leak of sensitive data. Automation is possible.

Threat Hunting- Threat hunting is a proactive approach or function of detecting and mitigating all the known and unknown threats in a system or networks. Automation is possible.

Security Operations- These are the practices and teams that are devoted to preventing, detecting, assessing, monitoring, and responding to cybersecurity threats and incidents. Automation is possible.

Data Sharing- Data sharing is a practice of sharing threat and vulnerability related data with other organization. Automation is possible.

File Integrity Checking- File Integrity Checking is a technology that monitors and detects file changes that could be indicative of a cyberattack. Automation is possible.

Password Cracking- Password cracking is a practice of breaking the password / passkey using some application. Automation is possible.

4. Conclusion

Attacks are growing exponentially, flourishing of IoT and 5G wireless technology offer more vulnerabilities to exploit. Some forums of cyber security technology include Artificial Intelligence and Machine Learning, Intrusion detection and prevention systems, Anti-malware, Next-generation firewalls, and a lot more. Securing assets helps in protecting national infrastructure, sensitive data, secret information, and national identities. Additionally, cyber security helps prevent cyber war. No doubt that automation helps in managing the repeated and tedious jobs. With the help of automation cyber security professionals can focus on other needful and important tasks. Big or small scale business can, too, integrate automation at every layer of their business operations. Here, in this work, we presented different cyber security jobs related to cyber security personnel. All the tasks described above are different from each other but the general idea remains same. The cyber security automation ecosystem is vast. There are different and critical jobs and those jobs can serve different purpose depending on the use case.

References

[1] Kemmerer, R. A. (2003). Cybersecurity 25th International Conference on Software Engineering, 705-715.

[2] Evans, M., Maglaras, L. A, He, Y. and Janicke, H. (2016). Human Behaviour as an aspect of cybersecurity assurance. Security and Communication Networks, 9:4667- 4679.

[3] Alotaibi, A., Furnell, S., Stengel, I. and Papadaki, M.(2016) A review of using gaming technology for cyber-security awareness. International Journal for Information Security Ressearch (IJISR), 6:660:666.

[4] Alkhudhayr, F., Alfarraj, S., Aljameeli, B. and Elkhdiri, S. (2019) Information Security:A Review of Information Security Issues and Techniques. 2nd International Conference on Computer Applications & Information Security (ICCAIS), 1-6.

[5] Donepudi, P. K(2015) Crossing Point of Artificial Intelligence in Cybersecurity. Am. j. trade poicy, 2:121-128.

[6] Mohammad, S. M and Lakshmisri, S. (2018) Security Automation in Information Technology. International Jouirnal Of Creative research Thoughts (IJCRT).

[7] Zhao, J., Shang, W., Wan, M. and Zeng, P. (2015) Penetration testing automation assessment method based on rule tree. IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 1829-1833.

[8] Gill, A. K, Zavarsky, P. and Swar, B. (2021) Automation of Security and Privacy Controls for Efficient Information Security Management. 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), 371-375.

[9] Harel, Y., Gal, I. B. and Elovici, Y. (2017) Cyber Security and the Role of Intelligent Systems in Addressing its Challenges. ACM transactions on Intelligent Systems, 8:1-12.

[10] Montesino, R. and Fenz, S. (2011) Automation Possibilities in Information Security Management. European Intelligence and Security Informatics Conference, 259-262.

[11] Aguirre, I. and Alonso, S. (2012) Improving the Automation of Security Information Management: A Collaborative Approach. IEEE Security & Privacy, 10:55-59.

[12] Lu, Y. and Xu L. D. (2019) Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. IEEE Internet of Things Journal, 6:2103-2115.

[13] Naik, S. and Maral, V. (2017) Cyber security — IoT 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 764-767.

[14] Sinha, A., Nguyen, T. H, Kar, D., Brown, M.,Tambe, M. and Xin Jiang A. (2015) From physical security to cybersecurity. Journal of Cybersecurity, 1:19-35.

[15] Tawde, R., Nivangune, A. and Sankhe, M. (2015) Cyber security in smart grid SCADA automation systems International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 1-5.