What are the potential cybersecurity vulnerabilities and cybersecurity risks associated with water treatment facilities in the United States, and how can machine learning reduce these risks?

Stephen C. Cobb

Old Dominion University

Abstract

This paper discusses to understand the cyber vulnerabilities and risks that are associated with water treatment facilities in the United States and how to reduce them through methods like machine learning and other safe measures. After doing research most vulnerabilities stem from the apps for employees to work at home, bad account security, and unsecure Internet of Things devices. Keeping up to date with cyber practices can be very hard and that is another reason why water treatment can be so vulnerable, but with the use of machine learning it does not have to be so rigorous. Training a model to look for the vulnerabilities above and all other common vulnerabilities in cybersecurity for water treatment is a really good way to stay safe and better responding to them than humans.

Keywords: Cybersecurity, Water Treatment, Machine Learning, Attacks, Vulnerabilities

Water treatment is a part of the United States critical infrastructure so understanding what are the cybersecurity vulnerabilities and risks that is has is very important. It is also important to understand how to defend against these vulnerabilities, one thing that could help is machine learning. The question this paper discusses is What are the potential cybersecurity vulnerabilities and cybersecurity risks associated with water treatment facilities in the United States, and how can machine learning reduce these risks? The three disciplines that is employed is water treatment, cybersecurity, and machine learning because water treatment is being studied for its cybersecurity and machine learning may be able to reduce the cybersecurity flaws. An interdisciplinary approach that helped me to research is thinking outside of the box and researching subtopics in each discipline. For instance, how do water treatment facilities operate on a day-to-day basis. This research relates to my major because it is they study of cyber vulnerabilities within a water treatment facility, and I also enjoy learning about Americas critical infrastructure.

Some key terms are cyber-attacks, cyber vulnerability, and algorithms. A cyber-attack is an attempt by a hacker to compromise, destroy, or damage data on a computer network system. A cyber vulnerability is a flaw in a computer system that can be exploited by a hacker to attack. In other words this is where hackers can start their attacks on systems. An algorithm in this paper is a machine learning algorithm and it is a way for computers to learn and make predictions from data. “Cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense,” (Biden).

Water treatment is very important, and they are becoming more digitized the reason that this is a disciplinary is because in this day it crosses roads with cybersecurity. Water treatment

facilities heavily rely on SCADA systems and industrial control systems to run different processes. Making sure these systems are protected is very important in order to prevent things like unauthorized access. “SCADA is usually implemented on manufacturing processes, (continuous and discrete manufacturing), treatment processes, (water and wastewater treatment), and distribution systems, (gas, oil and water pipelines). SCADA systems also perform monitoring, data logging, alarming and diagnostic functions so that large, complicated process systems can be operated in a safe manner. The SCADA system controls the sequencing and speed of pumps, and maintains run-time logs for maintenance scheduling,” (Andhare). Protecting the SCADA systems is important, but training and awareness is also important. Educating staff on cybersecurity like password improvement and phishing awareness is very important in order to reduce insider threats and human error.

Cybersecurity for water treatment is a must for the critical infrastructure industry in the United States. Everyone depends on clean water here. With cyber-attacks being on the rise opportunities do arise in water treatment facilities. Most cyber attacks are very basic through the use of normal cyber security practices like updates and other things will cause down time in systems and that is when attackers could come to light. There are three common cybersecurity threats in the water sector, and they are process control systems, insider threats, and external connections for remote access. Process control systems like SCADA which is a system that gathers real-time data and analyzes it is connected to multiple systems and if one of the connections are weak then that can cause a vulnerability. Insider threats are a real thing as well through the people who work closet to the systems, they know them the best and can create loopholes for less work and can lead to a vulnerability. They also can sell information for financial gain. Remote access to vendors and suppliers can create lack of physical security,

unauthorized access to systems, and eavesdropping which and lead to a lot of vulnerabilities like devices being stolen or even overlooking the screen. According to Germano (2018) “The effects of a cybersecurity attack on critical water sector operations could cause devastating harm to public health and safety, threaten national security and result in costly recovery and remediation efforts to address system issues as well as data loss.” In 2019 the WaterISAC made a guide of 15 fundamentals for cybersecurity for water treatment. “These 15 cybersecurity fundamentals will assist the water and wastewater utilities, and the critical infrastructure stakeholders (i.e. owners and operators) to prevent and minimize cases of cyber attacks in the water and wastewater utilities sector,” (Alabi, ect…). The best practices as of right now for cybersecurity for water treatment range from assessing risks and minimizing control exposer to collaborating with communities.

Machine learning is a type of artificial intelligence that is based off algorithms, and it can learn from data to preform without direct instructions. It can improve cybersecurity in a lot of ways like anomaly detection, predictive analysis, automated response, fraud detection, threat detection, and authentication. Anomaly detection is when machine learning is trained to see normal patterns and when something is off it can flag that as a threat or vulnerability. This has helped in the past recognize attacks like zero-day and insider threats that were unseen. Predictive analysis is when machine learning looks at the past history of data to predict future attacks. Through looking at patterns in the past machine learning can anticipate a threat and give the water treatment facility a heads up so they can correctly defend against an attack. Automated responses is when machine learning responds to a cyber related threat in real time. For instance, if there is suspicious activity on a system at the water treatment facility machine learning could just block that user and notify the security team on site. Fraud detection in machine learning is

when it detects fraud within the water treatment company through analyzing various data and user behavior. Threat detection, machine learning can go through huge amounts of data to see if there are any threats and put them into different categories. Things like phishing emails and other cyber-attacks. Machine learning can also make authentication better by looking at user behavioral patterns. This helps by detecting if there has been some sort of unauthorized access and creates a better authentication system. The main problem with machine learning and water treatment facilities is how to implement them throughout the nation. “While these successes have been noted, AI and ML applications are not without their challenges that must be overcome before widespread implementation occurs. This review offers a cross-section of mostly ML techniques, with some AI and smart technologies, that have been applied in water-based applications to optimize and model water- and wastewater-treatment processes (including chlorination, adsorption, and membrane-filtration processes), natural-systems monitoring, including dissolved-oxygen monitoring, water-quality-index monitoring and water-level monitoring, and water-based agriculture including hydroponics and aquaponics,” (Lowe, ect…). The use of machine learning has been researched globally as nations keep up with modernization.

There are three major findings disclosed in my interdisciplinary research on water treatment, cybersecurity, and machine learning. The first one is cyber-physical security of water treatment systems, since things are becoming more digitized the concern of physical cyber risks have grown as well. Interdisciplinary research that connects machine learning, cyber security specialists and water treatment experts can all help mitigate vulnerabilities in a water treatment plant. By using machine learning water treatment facilities can better the resilience against cyber threats. Machine learning can also predict maintenance of water treatment infrastructure that can

help prevent cyber-attacks and physical failures. Recognizing not normal behavior is also very important for detecting cyber threats. Interdisciplinary research that combines water treatment expertise, machine learning, and cybersecurity can help see what normal behavior and not normal behavior looks like.

One conflict that I found in my data is recognizing the actual degree of risks that a computer network withholds because questions must be asked like will a cyber-attack produce a physical effect? Since a water treatment plant is critical infrastructure, the answer is yes. "Infrastructures are robust and resilient, capable of absorbing damage without interrupting operations and accustomed to doing so after natural disasters, floods, or other extreme weather conditions. In short, the cyber threat to critical infrastructure has been overstated, particularly in the context of terrorism," (Lewis). Computers are here to stay, and everything is getting digitalized so more and more vulnerabilities will come so the United States need to plan accordingly for infrastructure protection. Taking risk assessments seriously is very important but is also difficult. Politics is one of the main reasons that cybersecurity is not taken as seriously because most do not understand computers. Another conflict that I found in my research is the cons of machine learning which is a type of artificial intelligence. One main point that I found was that machine learning can manipulate data and have malicious outcomes. If the water treatment plant is overseen by a machine learning model an attacker can learn the trained data set and poison it with malware and that can change the results. An attacker could also manipulate the data by using a bias injection. "Data injection refers to the manipulation of the value generated from sensors, actuators, and other devices, while the command 'injection' refers to changing server-issued instructions. The FDIA is one of the most common attacks and can be launched on any critical infrastructure by penetrating the communication sessions between

different devices. FDIAs can damage physical components, induce huge economic losses, and even create life-threatening scenarios [8,9]. Therefore, it is essential to prevent and detect FDIAs in any critical infrastructure," (Kumar, ect …). These two conflicts are important because politicians when it comes to cybersecurity do not do anything until something has already been attacked, and machine learning is very new so there are some problems with it still.

To construct a more comprehensive or complex understanding we must first understand how a water treatment plant works. Wastewater has a lot of random things in it ranging from food scraps and human waste to, gravel and chemicals. The cleaning of wastewater is a multi-step process that first requires filtering out the solids, the rest of the water is called effluent and goes through screens that get smaller as the water passes through to get out all the other particles. The next step is filtration which takes out all the bacteria by putting the water through sand filters. The final step is where the water is moved to tanks and chlorine is added to kill the remaining bacteria. After this the water is ready to go back into rivers. Computers help with this because they help with research and data. The computers also have a software that helps design the right system for the waters needs. Once everything is figured out by computers engineers are trained to make sure everything goes smoothly after that. Computers help with operational costs and productivity so protecting them are vital for the water treatment process and making sure this country remains healthy. The types of cyber-attacks on this critical infrastructure can be either DDoS attacks, ransomware, or malware and they can all be prevented by the measure above like making sure systems are constantly updated and looking into who is on the computer network at all times. Machine learning can help oversee some of this because it can constantly look for abnormal behaviors and report it to the cyber team. Also cybersecurity is a must these days and everything must be protected or else the worse could be expected to come.

In order to reflect on this theory tests can be run in a way where there is an unprotected network, a protected network, and. Protected network with the assist of machine learning. The findings are that the unprotected network is compromised and there is no data recovery because everything has already been taken and held up for Ransome. The protected network may be attacked or may not be, but if attacked it could be a small one where things are just getting monitored on the systems until the right time to extract data. Unless someone on the cyber defense team gets lucky and finds the hole where the attackers got in and understood what they did at an early stage then things should be okay, but often people do not know they are being attacked until it is too late. A protected network with the assistance of machine learning could be well off as it can catch abnormal behavior right as it happens and reported so water treatment companies should invest into it in the future.

To conclude about the research question What are the potential cybersecurity vulnerabilities and cybersecurity risks associated with water treatment facilities in the United States, and how can machine learning reduce these risks? Defending against vulnerabilities and attacks is the main task at hand because I am sure that if water treatment plants start getting attacked then the public will go into a state of fear. The three disciplines that were talked about were water treatment, cybersecurity, and machine learning because water treatment facilities could be more secure if things were properly guarded. The interdisciplinary approach that helped me the most was looking into subtopics because all three disciplines are very deep and complex. This research relates to my major because it is they study of cyber vulnerabilities within a water treatment facility, and I also enjoy learning about Americas critical infrastructure.

Works Cited

Alabi, M., Telukdarie, A., & Van Rensburg, N. J. (2020). *(PDF) cybersecurity and Water Utilities: Factors for influencing ...* researchgate. https://www.researchgate.net/publication/349849423_CYBERSECURITY_AND_WATER_UTILITIES_FACTORS_FOR_INFLUENCING_EFFECTIVE_CYBERSECURITY_IMPLEMENTATION_IN_WATER_SECTOR

Andhare, S. L. (2014, July 14). *Water treatment plant operating by using SCADA*. Asian Journal of Engineering and Technology Innovation. https://ijarsct.co.in/Paper1184.pdf

Biden, J. (2023, March 1). *National Cybersecurity strategy*. The White House. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Germano, J. H. (2019). *Cybersecurity Risk & Responsibility in the Water Sector*. AWWA. https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf?ver=2018-12-05-123319-013

Kumar, A., Saxena, N., Jung, S., & Choi, B. J. (2021, December 29). *Improving detection of false data injection attacks using machine learning with feature selection and oversampling*. MDPI. https://www.mdpi.com/1996-1073/15/1/212

Lewis, J. (2006, January). *Cybersecurity and Critical Infrastructure Protection*. Amazon Web Services. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/september_2006_menc.pdf

Lowe, Matthew, Ruwen Qin, and Xinwei Mao. 2022. "A Review on Machine Learning, Artificial Intelligence, and Smart Technology in Water Treatment and Monitoring" Water 14, no. 9: 1384. https://doi.org/10.3390/w14091384