Internet of Things for Water: Real-time Water Level Sensing to Support Flooding Emergency Management

Privacy and Security Risks from Cybersecurity Attacks on IoT Devices in Different Sectors

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Systems Engineering

By
Nicolas Khattar

October 27, 2022

Technical Team Members:
Andrew N. Bowman
Arnold Mai
Lily Malinowski
Khwanjira Phumphid
Taja M. Washington

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Rider W. Foley, Department of Engineering and Society
Victor A Leal Sobral, Department of Computer Science

Jonathan L. Goodall, Department of Engineering Systems and Environment

IoT for Preventing Flood Damages

Flooding and extreme rain events will be a top climate hazard for Charlottesville by 2050, according to a study made by Lopes and Tilman (2020). Climate change is causing temperatures and rainfall throughout the city of Charlottesville to surge. The frequency and severity of storms is increasing, magnifying the flooding impacts. The same shows that from 1995 to 2015, Charlottesville and Albemarle County experienced around one hundred floods that created more than a million dollars in damage. According to the National Oceanic and Atmospheric Administration (2022), the U.S. averages 5,000 floods each year, each of which poses a threat to lives and property. Steps need to be taken to address the crisis before flooding events further escalate and cause local and national emergencies. Although monitoring the floods does not solve the climate change issue, it is essential to prevent damage as it implements proactive measures for the community.

A report by Galloway et al. (2020) emphasizes that without proper monitoring systems, flooding will cause economic loss, social disruptions, and damage to the urban environment. In response to flooding, cities and towns around the world are currently looking for a precautionary measure to minimize adverse effects. A blog on the website Renkeer (2021) mentions that in view of the frequency and severity of floods, many technological companies are using the Internet of Things (IoT) to propose flood monitoring and early detection systems that allow administrations to prepare for floods in advance. IoT is a crucial part in the development of smart cities because it promises more ubiquitous environmental sensing capabilities (Goodall 2022). Among them, flood monitoring systems with sensors are widely used. When applied to water systems, the IoT device has the potential to increase insights into how hydrologic systems respond to extreme rainfall events, thus aiding in emergency management efforts before and during extreme weather events.

Based on an article from IoT for All (2022), floodwaters can rise quickly and with little warning, resulting in chaos for citizens and emergency response teams. IoT networks that monitor flood risk offer response teams real-time data and insight to detect potential flooding reducing the loss of life, property, and business. Deploying environmental sensors to measure water levels and tides is essential for a better understanding of the environment and how particular areas within a community like Charlottesville react to rain events. With the data collected from the sensors, the city can get an even deeper insight into when and where problems might occur, enabling them to enact preventative measures. To maintain the privacy and integrity of the data, an important aspect of the network, which is the cybersecurity risk should be addressed. Our team's aim is to improve the efficiency and security of Charlottesville's existing IoT water sensor infrastructure which provides real-time water level sensing to support flooding emergency management in the city.

Flood Monitoring and Cybersecurity Risks

Water level measurement techniques have vastly advanced since the end of the 20th century. Since then, the IoT technology has been widely adopted in all industries to become the most cost effective and efficient two-way communication of data. It is equipped with wireless sensors that leverage long range, low power technology to collect data and provide actionable insights to end-users to mitigate flood risks, as explained in an article written by Landsome (2022). Currently in Charlottesville, ten different battery powered IoT sensors are online. There are three different types of sensors used: water level, soil moisture, and rainfall, each purchased from the company Decent Lab. Our team is working on deploying three additional sensors near creeks close to affordable housing.

Every sensor is fixed to an IoT device of its own. The IoT device will be connected to the Internet through the LoRaWAN wireless protocol using Cisco wireless gateways located within a 10 km radius (Tan 2022). The IoT devices are managed by The Things Network (TTN), which is a LoRaWAN Network Server, and the data collected is stored in the Google Cloud platform. Finally, Grafana is a third-party Application Programming Interface (API) used to visualize real-time sensor data feeds, and to draw insights from the collected data to support decision-makers. Our project main goal is to find a correlation between soil moisture, rainfall, and water levels from the streams. This will create a flood risk model that predicts and incorporates anticipated environmental changes like stream-level rise, changing precipitation patterns, and warming sea surface and atmospheric temperatures (Davis 2022). This model will predict flood risks and help to develop initiative-taking actions in the future.

Other tasks our team members are working on are increasing the efficiency of the battery usage of the IoT devices, improving the user interface and experience to provide clearer data visualization, and my section which is reducing the risks of cybersecurity attacks to prevent a data breach, or to avert an intruder from shutting down the flood monitoring system. The latter raises several alarming questions regarding the privacy and security of the IoT network and how stakeholders involved could be affected. Whenever someone uses a smartphone app to get directions, make reservations, share photos, purchase tickets, or check email, they are using APIs (Jablonski 2019). According to an article written by Gartner (2020), it is predicted that in 2022, API abuses will become the most-frequent attack resulting in data breaches for enterprise web applications. The same research estimated that 52 % of the APIs adopted by companies are from third parties. The rapid rise of new integrations between third-party cloud apps and core systems puts pressure on traditional third-party review processes which overwhelms the security teams. If these integrations proliferate without sufficient understanding and mitigation of the specific threats they pose, attacks are bound to keep happening, according to an article in Venture Beat (2022). To avoid this, I will be looking at all the several types of cybersecurity attacks that could potentially infiltrate the IoT infrastructure from every possible node. Then, I will analyze the current security protocols already setup to find the weak spots and propose recommendations to secure the network. Overall, this highlights the major responsibility the IT department has towards preparing for cybersecurity attacks of third-party APIs to protect the privacy of the data secured. It also shows how relevant the third-party API abuse is bound to happen in the future to any business size.

Privacy and Security Risks of Third-Party APIs for Flood Monitoring

We cannot understand how societies work without an understanding of how technologies shape our everyday lives. IoT devices changed all kinds of industries in the world and redefined what was possible. This technology offers an equilibrium between the digital and physical world by connecting them together. This relationship can be described by the Actor-Network Theory (ANT) which consists of a network of human and non-human actors that connect together. ANT fits right in the middle of social constructivism and technology determinism. Latnal (1999) describes it as: "It explores the ways that the networks of relations come into being, how they are maintained, how they compete with other networks. It examines how actors enlist other actors into their world and how they bestow qualities on these actors." In the past non-human actors have needed humans to interact with each other, but this is not the case anymore. Now in the IoT, the Internet, a non-human actor is the connector that facilitates the interactions between the

Things in the network. While IoT devices are deliberately activated by humans during the setup phase, in some cases they are not directly human-initiated and need non-human input to operate. For example, automatic alarms for floods are initiated by a non-human actor. Adding a new actor, such as the IoT device into the organization, will affect the functioning of the entire network.

Intermediaries are platforms that advertise properties and link different actors together. The third-party API Grafana is the intermediary that creates relationships between the management monitoring the data and the IoT devices collecting the data. In some networks, delegation reconfigures the organization of process by transforming how results are achieved. Before tools like Grafana existed, the IT engineers had to manually extract the data from the cloud, then write a code to graph the different water levels. The process was then delegated to Grafana which reduced human error and converted it to a more efficient network. According to Latour (1988), an inscription device is any set-up, which provides a visual display of any sort in a scientific text to makes the perceptive judgment simpler. The inscription device here is Grafana, because it provides graphs for the management to base decisions on. Grafana is the hardest to control because it oversees an enormous amount of data. Due to the highly connected nature of the technology, involving inadequate levels of security, data can be leaked. Setting aside the financial damages, leaks are a breach of the privacy of data owned by companies or organizations which, in such cases, is the team's sponsor, Commonwealth Cyber Initiative.

These data and other personal information generated by IoT devices can potentially be sold for advertising and data harvesting purposes. Attention has been drawn by Lupton (2020) to the risk of IoT-generated data being used for government surveillance purposes, and cyber criminals could be hacking these data for discrimination against marginalized social groups.

Cybersecurity attacks on all sectors continue to rise as these platforms are becoming more essential. A virus can contain ransomware, which can shut out or erase data, making an emergency decision impossible until the information can be restored or until technicians perform physical tests on the site. If, for instance, IoT sensors are targeted, and inaccurate data is communicated to the responsible authorities, the proper evacuation procedures and alarms will not take place. This false emergency causes widespread panic in society, alongside financial damages from problems including fraudulent flood assistance payments. According to an article by Lupton (2020), Saudi Aramco, the world's largest producer of petroleum and natural gas products, faces a $50 million ransom. The stolen data, held by third-party contractors, included employees' profiles, company information and customer invoices. This ransomware demonstrates the financial damages caused by cybersecurity attacks which also entail the breach of privacy of employees.

Authorities should release guidance outlining the permitted verification types for third-party app privacy and security while enabling the provider organizations themselves to undertake an appropriate level of review of a third-party app before permitting it to connect to their APIs. Security officials recommend developing an accreditation regulating the privacy and security of third-party apps that want to connect to certified health IT APIs. Regulations provide guidance to verify the security and privacy of third-party apps. They should exist to responsibly manage the customer's data and to notify them of any change including, a cybersecurity attack.

Research Question and Methods

How is privacy and security affected by cybersecurity attacks on the third-party APIs of IoT devices used in flood monitoring? Vinugayathri (2022) mentions in his article that IoT delivers constant feedback and facilitates better decision-making for businesses. However, cybersecurity attacks continue to rise as these platforms are spreading everywhere. Hackers can infiltrate viruses that can do more than slow down or corrupt a network. The IT and security teams need to be trained and ready for any attack. The privacy of the employee and the integrity of the data generated for flood monitoring is at stake.

The issue will be tackled by looking at all the different privacy risks of APIs in environmental businesses. I plan to collect information by conducting interviews with professors at UVA specialized in cybersecurity namely Wajih Ul Hassan, Yuan Tian, and Jack Davidson to find the common weak spots in API networks. I will also review news articles from 2018 until now to register all the different events capturing third-party API cyberattacks. Some of these reports are published by major pioneers in cybersecurity like "Cool Vendors in API Strategy" from Gartner, "Global Security Report" from Trustwave, and "OWASP API Security Top 10" from OWASP. After analyzing the topic with all the input available, I will interpret and assess the data by reviewing every source carefully and noting the main privacy concerns of third-party apps that want to connect to APIs of IoT devices.

Secure Network Ready for Flooding Monitoring

Big industries are facing privacy and security issues due to cybersecurity attacks on the third-party APIs of IoT devices used in their businesses. According to the Ponemon Institute, 51% of organizations acquire IoT products through a third party; meanwhile, 48% of organizations have been subject to at least one IoT attack, and that number is rising. Although the cybersecurity risks of hacking the API of an IoT flood monitoring device do not have the same financial effect seen in cybersecurity attacks on APIs used in the Oil and Gas industries, cyberattacks can still lead to a breach of data of the company and cause public panic. Relationships between management and IoT sensor devices are derived from this intermediary, the API. This mediator is the hardest to control because it creates live insights and generates an enormous amount of data. A leak can occur due to many issues, one of them being that the sensors were introduced without adequate levels of security testing which causes several ransomware attacks. Financial damage is caused by a data breach of the company and employees' privacy. This needs to be addressed today to prevent future major human catastrophes and huge financial losses. I plan to develop a certification framework that covers all possible scenarios of data breach. My goal is to regulate the privacy and security of third-party apps that want to connect to APIs of IoT devices. All the analysis will ensure that the network never collapses, or information is dissipated to unauthorized users. The IoT system will always be alerted to send notifications in case of floods, to avoid as many casualties as possible.

References

Admin, R. (2021, September 25). Flood monitoring system with IOT Sensors. Retrieved October 15, 2022, from https://www.renkeer.com/flood-monitoring-system-with-iot-sensors/

Alon Jackson, A. (2022, August 21). Third-party app attacks: Lessons for the next Cybersecurity Frontier. Retrieved October 15, 2022, from https://venturebeat.com/security/third-party-app-attacks-lessons-for-the-next-cybersecurity-frontier/

Bijker, W. E., &amp; Law, J. (1992). ‘‘Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts’’. In Shaping Technology/Building Society: Studies in Sociotechnical Change. Cambridge, MA: MIT Press.

Davis, M. (2022, June 20). Flood risk models vary widely - here's what you need to know (and how to mitigate threats). Retrieved October 15, 2022, from https://www.valuepenguin.com/flood-risk-study

Galloway, G. E., Reilly, A., Ryoo, S., Riley, A., Haslam, M., Brody, S., . . . Parker, S. (2018). The growing threat of urban flooding: 2018 [Scholarly project]. Retrieved October 14, 2022, from https://today.tamu.edu/wp-content/uploads/sites/4/2018/11/Urban-flooding-report-online.pdf

Goodall, J. (2022, August 22). UVA CollabSYS4055ResourcesCapstoneProjectDescriptions [2022-2023 SYS Capstone Project Descriptions]. Charlottesville.

The Internet of Things (IoT): A New Era of ThirdParty Risk (Rep.). (2017, May). Retrieved October 14, 2022, from Ponemon Institute LLC website: https://www.ponemon.org/local/upload/file/IoT%20and%20Third%20Party%20Risk%20Final1.pdf

IOT is eating the world: Apis and rest. (2020, June 01). Retrieved October 16, 2022, from https://www.iotforall.com/iot-rest-api

Jablonski, F. (2021, November 20). The biggest security risks of using 3rd party apis. Retrieved October 15, 2022, from https://www.ipswitch.com/blog/the-biggest-security-risks-of-using-3rd-party-apis

Lansdowne, R. (2002, February 4). IOT technology mitigates flood, Climate Change Effects. Retrieved October 27, 2022, from https://www.estormwater.com/sewers-drainage-systems/flood-control/article/10983615/iot-technology-mitigates-flood-climate-change-effects

Latour, B. (1988). *Science in action: How to follow scientists and engineers through society*. Harvard.

Lopes, C., &amp; Tilman, G. (2020, June). Local effects of climate change (Rep.). Retrieved October 22, 2022, from Community Climate Collaborative website: https://static1.squarespace.com/static/5a0c67f5f09ca475c85d7686/t/5efe15db11d5fa0d7fffd167/1593710045709/Local+Effects+of+Climate+Change.pdf.

Lupton, D. (2020). The internet of things: Social dimensions. *Sociology Compass, 14*(4). doi:10.1111/soc4.12770

Morgan, L. (2022, October 17). IOTW: Contractor allegedly responsible for aramco $50 million ransom. Retrieved October 15, 2022, from https://www.cshub.com/executive-decisions/articles/iotw-contractor-allegedly-responsible-for-aramco-50-million-ransom

Pillai, S., Malinverno, P., O'Neil, M., & D'Hoinne, J. (2020). Cool Vendors in API Strategy. Retrieved October. Retrieved October 15, 2022, from https://www.gartner.com/document/3985290

Semtech. (2021, July 13). Preventing flood damage with IOT Sensors. Retrieved October 151, 2022, from https://www.iotforall.com/preventing-flood-damage-with-iot-sensors

Smith, A. B. (2022, January 24). 2021 U.S. billion-dollar weather and climate disasters in historical context. Retrieved October 14, 2022, from https://www.climate.gov/news-features/blogs/beyond-data/2021-us-billion-dollar-weather-and-climate-disasters-historical

Tan, J. (2022, July 22). Lorawan gateways - what you need to know! Retrieved October 15, 2022, from https://www.seeedstudio.com/blog/2021/06/12/lorawan-gateways-what-you-need-to-know/

Tatnall, A., & Gilding, A. (1999). Actor-Network Theory and Information Systems Research.

Vinugayathri. (2020). Top 10 ways IOT is transforming the businesses today. Retrieved October 16, 2022, from https://www.clariontech.com/blog/top-10-ways-iot-is-transforming-the-businesses-today