Module 2: Critical Thinking

Use Case for Smart Governance

Nolan Byrnes

CSC510 – Foundations of Artificial Intelligence

Colorado State University – Global Campus

Professor Bingdong Li

May 27th, 2023

Module 2: Critical Thinking

Oracle defines the Internet of Things (IoT) as “the network of physical objects—‘things’—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet” (Oracle, 20xx, para. 1). Sharda mentions that some of the benefits that come with the IoT is that it “reduces cost by automating processes”, “identifies problems quickly”, and "Enables better decision making based on real-time information" (Sharda et. al., 2019, pg. 695). This paper explores the advantages that IoT can be used to enhance smart governance some of the challenges that they face, and suggestions on how the challenges can be overcome.

Enhancing Smart Governance with IoT Technologies

Cameras are used to allow the public to see the road conditions. For example, The Texas Department of Transportation has a [site to view all of the live traffic cameras](https://www.txdot.gov/discover/live-traffic-cameras.html) which is open to the public to view (Texas Department of Transportation, n.d.). An AI solution using computer vision could monitor the feeds of all the cameras, and alert authorities when a crash has been detected on the highway, monitor traffic speed, or if the road is not in a safe condition to drive. Using AI on the cameras can help plan routes and determine travel times. Furthermore, an AI solution which takes data from the public cameras can allow authorities to be alerted of any accidents when they occur, and what they may need to send to a scene. They may need to send more resources if an 18-wheeler overturned compared to a fender bender. These automated alerts the AI solution would send can improve response time to accidents, clearing the traffic and keeping the public safe.

The [National Weather Service has weather stations](https://forecast.weather.gov/stations.php?foo=0) across the country that report metrics such as wind speed, temperature, and humidity levels (National Weather Service, n.d.).

The weather stations that are deployed help the National Weather Service alert the public when dangerous weather conditions are occurring. An AI solution could be used with the data that is collected by these sensors to better predict when and where bad weather will occur. With the advanced warnings, this can give more time for the public to be prepared in the case of life-threatening weather events.

An AI solution that is implemented on cameras placed in public settings such as schools can help maintain public safety by detecting when an individual is holding a gun. With cameras being placed in schools and other public settings, we could use computer vision to detect when an individual is carrying a gun, and alert authorities as soon as it is detected, and could even lock doors to prevent the individual from progressing further into the building. Implementing an AI solution that detects possible threats could allow authorities to respond quicker, and possibly intervene before incidents occur.

Challenges of Smart Governance

One challenge that smart governance may need to overcome when using IoT devices is cybersecurity. Any device that is connected to the internet has a risk of being compromised by bad actors. A botnet attack called Mirai took advantage of Iot devices by scanning the internet for open telnet ports, then attempt to log in by “using 61 username/password combos that are frequently used as the default for these devices and never changed” (Fruhlinger, 2018, para. 7). By doing so, Mirai had a botnet that would perform DDoS attacks. To prevent IoT devices from being compromised, every IoT device should not use the default username/password combination. Keeping devices updated could also prevent the IoT devices from being compromised. Setting up cron jobs on IoT devices to automatically update on a regular basis is another way to help keep the IoT devices secure from being used by bad actors.

Kankanhalli mentions that another challenge for IoT and AI for smart government is related to the energy consumption that the IoT-enabled AI applications use (Kankanhalli, 2019, para. 13). With an estimated 20-50 billion IoT devices being connected to the internet by 2025, the amount of power that these devices use collectively must be considered (Sharda et. al., 2019, pg. 695). Between the IoT devices that are powered by batteries and ones connected directly to a power source, it takes a lot of energy and resources to keep the devices powered due to the amount of IoT devices that are out there. IoT devices such as outdoor cameras could use solar power with a rechargeable battery. IoT devices could also conserve energy by collecting data at a slower pace. For example, cameras monitoring traffic conditions may not need to record a live feed of the traffic, so they could send images at a slower rate, such as every 30 seconds, reducing the amount of data that is being sent and conserving energy.

Another challenge that smart governance needs to overcome when using IoT devices is the issue of malfunctions and false positives. If weather sensors are malfunctioning, bad data could be returned and potentially make it seem that a particular area is experiencing bad weather when it is not. If an AI solution is implemented to detect when an individual is holding a firearm in an unauthorized area, if the program misidentifies an umbrella as a firearm, the program could send out a false positive. IoT devices must be maintained to make sure that the data that it is receiving and sending is accurate. Furthermore, for situations where an IoT device is reporting a crash on a highway or an individual with a firearm, video feed could be sent to a dispatcher so that we can have a human make the final judgement, to help prevent bad judgements from being made automatically.

Privacy is another challenge that smart governance must overcome when using IoT devices. Open Access Government suggests that using privacy by design principles which “involves designing systems and processes that protect data privacy from the very beginning, rather than trying to add privacy measures after the fact” (Open Access Government, 2023, para. 5). Placing traffic cameras high enough to where cars can be seen, but license plates and faces can not be identified could be an example of this, since identifying individuals in the camera feeds is not the intention for the cameras usage. For cameras that are being used to monitor for firearms in unauthorized areas, video feed should not be saved or sent anywhere from the device unless the camera is detecting criminal activity. By using a privacy be design approach, can help ensure that the privacy of the public is maintained, and the data collected by the IoT devices is not being used in ways that it was not intended to.

Conclusion

Smart governance can keep the public informed of weather and traffic conditions as well as keeping the public safe from criminal activity, but also comes with challenges that must be addressed. By having a privacy by design approach to the implementation of the IoT devices, we can protect the privacy of the public. Having traffic cameras set high enough not to identify license plates and only recording video feeds when criminal activity is being witnessed keeps the data being collected from being misused. To prevent IoT devices from consuming too much energy, solar panels should be used wherever applicable, and the rate of which the data is being sent should be at a rate that is reasonable for the use case. Consistent inspections of the IoT devices are necessary to make sure that the data that is being collected is accurate, and we should have a human in the loop when major events are being reported by the IoT devices to prevent false positives from occurring, which would decrease the public’s trust in the systems in place.

**REFERENCES**

Fruhlinger, J. (2018, March 9). The Mirai botnet explained: How IoT devices almost brought down the internet. CSO Online. <https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html>

Kankanhalli, A., Charalabidis, Y., & Mellouli, S. (2019). IoT and AI for smart government: A research agenda. (2019). Government Information Quarterly, 36(2), 304-309. <https://doi.org/10.1016/j.giq.2019.02.003>

National Weather Service. (n.d.). National weather service : Observed weather stations. <https://forecast.weather.gov/stations.php?foo=0>

Open Access Government. (2023, February 9). The importance of data privacy in smart cities. <https://www.openaccessgovernment.org/importance-data-privacy-smart-cities/152918/>

Oracle. (n.d.). What is the Internet of things (IoT)? Oracle | Cloud Applications and Cloud Platform. <https://www.oracle.com/internet-of-things/what-is-iot/>

Sharda, R. D., & Delen, D. (2019). Analytics, Data Science, & Artificial Intelligence (11th ed.). Pearson.

Texas Department of Transportation. (n.d.). See live traffic cameras. <https://www.txdot.gov/discover/live-traffic-cameras.html>