PropTech Cases
CASE STUDY LIBRARY

This Photo by Unknown Author is licensed under CC BY

INSIDE THIS ISSUE

Issue No. 2022-09

Editor: Edward Yiu – Associate Professor, University of Auckland Business School, New Zealand. edward.yiu@auckland.ac.nz

PRIVACY V. CONVENIENCE

SMART BUILDINGS – HOW TO STRIKE A BALANCE BETWEEN PRIVACY AND CONVENIENCE?

Innovations in Smart Buildings have bought convenience and efficiency to occupants, such as smart lifts and smart HVAC. However, with the powerful predictive analytics in smart buildings, they can recognise the identities of all occupants to analyse the occupants' behavioral patterns. The trained systems can then provide individualised optimal services, but the privacy of the occupants may be compromised. A case of a smart lift is provided which can recognise users' faces and share the users' personal identity information with the IoT-enabled cloud to check the users' authorisation and run the machine learning model algorithm to identify the destination floor of the users. An article by Groth (2022) on IoT ethics is also provided for reference.

Groth, Diane (2022) IoT ethics must factor into privacy and security discussions, TechTarget, January 6.

JESSICA HUO'S REPORT

BLOCKCHAIN INTEGRATION

IoT sensors are a core component of smart buildings. Sensors are the devices that monitor and record the environment data, sending it off to a computer processor (IotaComm, 2019). The IoT devices will monitor building characteristics, analyse the data and produce insights around occupants' usage patterns and trends, which can be used to improve the building environment and operations (IotaComm, 2020).

This undoubtedly creates undeniable convenience as smart infrastructure management includes automated parking systems, water usage control, elevators, conference rooms and much more, leading to potential cost savings and better space management (Woolpert, n.d.). However, this leads to concerns with privacy as a wide range of user data is collected.

One way to strike a balance between privacy and convenience of smart buildings is to increase privacy and security by integrating blockchain secure interfaces into IoT devices. IoT devices have insufficient computing capacity to support robust protection and encryption algorithms (Šarac et al., 2021). IoT's main challenges are security vulnerabilities, privacy and lack of industry standards. Blockchain integration can provide decentralisation and authentication, adding anonymity and versatility to the IoT infrastructure. This solution enhances the reliability of data sent to remote services as cryptographic algorithms will be applied to encrypt and decrypt data to ensure it's kept private and secure before it is sent. Blockchain will also eliminate single control authority and IoT devices' historical transaction records and provides trust between devices.

CASE: SAUTER - BLOCKCHAIN TECHNOLOGY FOR DATA INTEGRITY

SAUTER specialises in building automation and system integration. SAUTER's intelligent building automation ensures optimal room climate with automatic control, optimisation, monitoring and regulation. They offer a security-oriented solution for the challenges IoT faces by creating a blockchain designed for data integrity in building automation (SAUTER, n.d.). The use of blockchain technology will protect the data and processes used in building automation (Sirus, n.d.).

This newly developed concept to protect the data integrity of automation stations features:

- Blockchain technology
- Monitoring data integrity of each station
- Detection of unintentional and intentional data alterations
- Data integrity breaches notification
- Immediate restoration of original datasets

SAUTER blockchain ring is created with data from automation stations in the building network. Each automation station uses its data to form a block in the chain and generates its own digital fingerprint. If there is a breach of the blockchain's integrity, the SAUTER's system responses are to trigger an alarm and send an email notifying of integrity violation. The affected automation station will be isolated, initiate automatic self-repair for automatic restoration and reintegrated into the building network. In order to isolate the affected stations, the creation of digital twins is required for every station. The digital twin is a copy of all static data stored in an encrypted database.

REFERENCES

IotaComm. (2019, March 12). The 4 components that make a smart building ecosystem. *Iota Communications, Inc*. https://www.iotacommunications.com/blog/the-4-components-that-make-a-smart-building-ecosystem/

IotaComm. (2020, October 6). What is a smart building? (The ultimate guide). *Iota Communications, Inc*. https://www.iotacommunications.com/blog/smart-building/

Woolpert. (n.d.). The smart building advantage: Comfort, safety, convenience and responsiveness. *Woolpert*. https://woolpert.com/news/blogs/the-smart-building-advantage-comfort-safety-convenience-and-responsiveness/#:~:text=A%20%E2%80%9Cdigital%20twin%E2%80%9D%20of%20the,emergency%20personnel%20to%20trouble%20spots.&text=Convenience.,elevators%2C%20escalators%20and%20conference%20rooms

Šarac, M., Pavlović, N., Bacanin, N., Al-Turjman, F., & Adamović, S. (2021). Increasing privacy and security by integrating a blockchain secure interface into an IoT device security gateway architecture. *Energy Reports*, *7*, 8075-8082. https://doi.org/10.1016/j.egyr.2021.07.078

SAUTER. (n.d.). *Building network security*. sauter-controls.com. https://www.sauter-controls.com/en/building-network-security/

Sirus. (n.d.). *SAUTER blockchain technology for building automation*. https://sirusinternational.com/sauter-blockchain-technology-for-building-automation/

RUTH ARVIDSON'S REPORT

CASES OF ALEXA AND SIRI

Privacy and convenience in smart buildings can be balanced by **ensuring transparency and accountability from organisations** who provide the smart devices (Groth, 2022).

Home voice assistants such as Amazon's Alexa and Apple's Siri provide huge convenience by listening for your voice activated actions to the internet and your devices at all times.

Amazon's business model relies on their gathering information about you for micro target advertising (Lynskey, 2019). They are not clear that Alexa can record your speech, age, gender, health, intoxication, personality, and an analysis of the environment - for example, glass breaking. This data provides huge commercial benefits (Lynskey, 2019). Amazon, have also been known to provide law enforcement agencies data - like Alexa's recordings – for criminal investigations (The Conversation, 2022).

Apple is more transparent in their process of handling Siri's data. Their profits do not rely on data collection and they use in-device computation and encryption at both ends. However, Siri is not as reliable a home assistant because of this (Lynskey, 2019).

Siri and Alexa are smart building Internet of Things (IoT) devices. The IoT device number is likely to triple from 2020 to 2030, resulting in the collection and sharing of more data (Groth, 2022). Apple, as above, are protecting the privacy of their customers, but they are lacking in some convenience features. Meanwhile, Amazon, as above, is lacking privacy but they are excelling at providing convenience. Companies need to strike the balance between these two illustrations. Organisations need to clearly outline their plans to handle personal information and they need to be honest about what information is actually being recorded (Groth, 2022).

CASE OF DECODE

The convenience of smart buildings may be able to be balanced with user privacy by using systems similar to Decode's technology.

We like the convenience that IoT is providing, however, IoT devices gather huge amounts of data. Now, much personal information is no longer private.

Technology similar to the Decode projects may protect users' privacy.

- Decode pilots were rolled out in Barcelona and Amsterdam from 2017-2019 by the European Union (EU).
- The pilot technologies let customers decide if they would keep their personal information private or share it for product improvement and other communal uses.
- They provided appropriate privacy protections for the information that users did choose to share.
- They gave innovators, local communities, and more a way to benefit from data rather than just the few monopolies that currently have access (DECODE, 2017).
- One example of their technology testing was during their Amsterdam pilot.
    - *GebiedOnline* (Neighbourhood online) was a neighbourhood social network that required login via email and password or Facebook login. The pilot instead created and tried an access system based off Attribute Based Credentials, to avoid the security issues of logging in the other way (DECODE, 2020).

Decode is providing great examples of technology that gives users' better understanding and control over their personal information. It shows, there is a balance possible between user convenience and user privacy. The balance needs government backing like Decode's EU to create the technology needed. Currently, some large organisations hugely benefit from the private information they gather (Google, Amazon, etc.), so there will be great resistance against creating this balance.

REFERENCES

The Conversation. (2022, July 15). Virtual assistants like Siri and Alexa are listening to children and then using the data. Newshub. https://www.newshub.co.nz/home/technology/2022/07/virtual-assistants-like-siri-and-alexa-are-listening-to-children-and-then-using-the-data.html

Groth, D. (2022, January 6). IoT ethics must factor into privacy and security discussions. Tech Target. https://www.techtarget.com/iotagenda/opinion/IoT-ethics-must-factor-into-privacy-and-security-discussions

Lynskey, D. (2019, October 9). 'Alexa, are you invading my privacy?' – the dark side of our voice assistants. The Guardian. https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants

DECODE. (2017, May 15). *What is DECODE?* https://decodeproject.eu/what-decode.html
DECODE. (2020, February 17). *Pilots*. Retrieved August 15, 2022, from https://decodeproject.eu/pilots.html