การระบุตัวตนของอุปกรณ์ไอโอทีโดยใช้การวิเคราะห์การรับส่งข้อมูลเครือข่าย

ณัฐพนธ์ อิทธินิรันดร[1*], โสภณ มงคลลักษมี[2]

บทคัดย่อ

การใช้งานอุปกรณ์ไอโอที (IoT) มีความนิยมสูงขึ้น ด้วยปริมาณการใช้งานที่เพิ่มขึ้นนี้ ส่งผลโดยตรงต่อการบริหารและความปลอดภัย เพื่อรองรับกับปัญหาดังกล่าว งานวิจัยนี้นำเสนอการแยกแยะอุปกรณ์ไอโอทีด้วยข้อมูลทางเครือข่ายในระดับ Network Layer และ Transport Layer โดยใช้การเรียนรู้ของเครื่องซึ่งช่วยรักษาความเป็นส่วนตัวของข้อมูลผู้ใช้งานและการแยกแยะอุปกรณ์อย่างมีประสิทธิภาพ ข้อมูลเครือข่ายของอุปกรณ์จะถูกจัดเก็บและสกัดข้อมูลทางสถิติที่จำเป็นในช่วงเวลา 10 นาที ซึ่งประกอบด้วยข้อมูลเช่น ขนาดแพคเก็ต จำนวนแพคเก็ต และพฤติกรรมของ IPID โดยข้อมูลที่ได้จะถูกนำมาใช้ในการเรียนรู้ของเครื่อง ซึ่งมีวิธีการเรียนรู้ที่ใช้คือ K-Nearest Neighbors, Naïve Bayesian, Random Forest, และ Support Vector Machine ในการวัดผลใช้ตัวชี้วัดที่ประกอบด้วย Accuracy, Precision, Recall, และ F-1 พบว่าค่าผลเฉลี่ยสูงกว่า 0.9 ในทุกด้าน นอกจากนี้ การใช้ข้อมูลพฤติกรรมของ IPID สามารถเพิ่มประสิทธิภาพได้ โดยเฉพาะเมื่อใช้ร่วมกับ Naïve Bayesian ซึ่งให้ผลดีขึ้นเฉลี่ยถึง 0.08 ในทุกตัวชี้วัด

คำสำคัญ : อุปกรณ์ไอโอที, การเรียนรู้ของเครื่อง, การจำแนก, การจัดการเครือข่าย

---

[1] หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิทยาการข้อมูล คณะวิทยาศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ กรุงเทพฯ 10110

[2] คณะวิทยาศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ กรุงเทพฯ 10110

* Corresponding author: Tel.: E-mail address: nuttapol.itti@g.swu.ac.th

IoT DEVICE IDENTIFICATION USING NETWORK TRAFFIC ANALYSIS

Nuttapol Ittinirundorn[1*], Sophon Mongkolluksamee[2]

Abstract

The popularity of Internet of Things (IoT) devices has increased significantly, directly impacting management and security. Therefore, this research proposes a method to classify IoT devices using network-level and transport-level data, combined with machine learning techniques. This approach helps maintain user data privacy and enables rapid device classification. The network data from devices is collected and statistically analyzed over a ten-minute period, including packet size, packet count, and IPID behavior. The collected data is used to train four types of machine learning models: K-Nearest Neighbours, Naïve Bayesian, Random Forest, and Support Vector Machine. The performance evaluation used accuracy, precision, recall, and F-1 measures, with average scores exceeding 0.9 in all aspects. Furthermore, incorporating IPID behavior data improved effectiveness, particularly when combined with Naïve Bayesian, resulting in an average improvement of 0.08 across all evaluation metrics.

Keywords : IoT Devices, Machine learning, Classification, Network management

---

[1] Data Science, Faculty of Science, Srinakharinwirot University, Bangkok, 10110, Thailand

[2] Faculty of Science, Srinakharinwirot University, Bangkok, 10110, Thailand

* Corresponding author: Tel.: E-mail address: nuttapol.itti@g.swu.ac.th

บทนำ

อุปกรณ์ไอโอที(IoT: Internet of Things) (Al-Qaseemi et al., 2016) หรืออุปกรณ์อินเตอร์เน็ตของสรรพสิ่งนั้น ในปัจจุบันได้เข้ามามีบทบาทอยากมากต่อผู้คน อุปกรณ์เหล่านี้ถูกติดตั้งและใช้งานเพื่อสนับสนุนการใช้ชีวิตประจำวันและการทำงานด้วยอุปกรณ์มีขนาดเล็กและการติดตั้งได้ง่าย อุปกรณ์เหล่านี้อาจถูกติดตั้งและใช้งานโดยไม่ได้รับการตรวจสอบและลงทะเบียน ซึ่งอาจมีผลกระทบต่อการบริหารจัดการระบบเครือข่ายรวมถึงด้านความปลอดภัยของภายในระบบเครือข่าย

อุปกรณ์ IoT นั้นถูกผลิตออกมาเพื่อตอบสนองต่อความต้องการที่สูงขึ้นอย่างรวดเร็วของผู้ใช้ อีกทั้งด้วยเรื่องของ IoT ยังเป็นเรื่องใหม่ทำให้ยังขาดแคลนองค์กรในการตรวจสอบและรับประกันคุณภาพของอุปกรณ์ IoT ส่งผลให้อุปกรณ์ IoT ในปัจจุบันยังคงมีความเสี่ยงสูงในเรื่องของความปลอดภัย ทำให้มีความเสียงสูงในการเกิดภัยคุกคามกับองค์กรที่นำอุปกรณ์มาใช้งาน อุปกรณ์ดังกล่าวนั้นสามารถสร้างความเสียหายให้กับระบบเครือข่ายหรือข้อมูลขององค์กรได้ เช่น การโจรกรรมข้อมูลที่มีความสำคัญต่อองค์กร การก่อกวนระบบเครือข่ายขององค์กรเพื่อให้สามารถดำเนินการช้าลง หรือไม่สามารถดำเนินการใดๆ ภายใต้เครือข่ายขององค์กรที่ถูกโจมได้ โดยอุปกรณ์ IoT โดยส่วนใหญ่จะมีขนาดเล็กและสามารถซ่อนตามสถานที่ต่างๆได้ และยากต่อการสังเกตุ ดังนั้นหากสามารถแยกแยะอุปกรณ์ IoT ได้ด้วยข้อมูลเครือข่ายที่พวกมันใช้ในการสื่อสารย่อมเป็นผลดีอย่างมากในด้านความมั่นคงปลอดภัย จึงควรสร้างคุณภาพในการให้บริการ หรือ Quality of Service (QoS) ด้วยวิธีการจำแนกอุปกรณ์ (Al-Qaseemi et al., 2016; Aluthge, 2017; Apthorpe et al., 2017; Meidan, Bohadana, Shabtai, Guarnizo, et al., 2017; Meidan, Bohadana, Shabtai, Ochoa, et al., 2017; Sivanathan et al., 2019; Sivanathan et al., 2017) ขึ้นเพื่อรักษาเสถียรภาพและคงไว้ซึ่งคุณภาพของการบริการเครือข่าย

ความรู้และงานวิจัยที่เกี่ยวข้อง

พฤติกรรมและลักษณะของ IP Identification

ในเลเยอร์ IP (Internet Protocol) Identification (หรือ ID) หมายถึงฟิลด์ภายในส่วนหัวของ IP ที่ช่วยระบุและประกอบแพกเก็ต IP ที่กระจัดกระจายกลับมาอีกครั้ง เมื่อข้อมูลถูกส่งผ่านเครือข่าย IP ข้อมูลจะถูกแบ่งออกเป็นหน่วยเล็กๆ เรียกว่า IP แพกเก็ต แพกเก็ตเหล่านี้อาจต้องถูกแยกส่วนออกเป็นชิ้นเล็กๆ หากขนาดของแพกเก็ตเกินหน่วยส่งข้อมูลสูงสุด (MTU) ของเครือข่าย ID ฟิลด์มีขนาด 16 บิตที่ไม่ซ้ำกันในแต่ละ IP แพ็กเก็ต หาก IP แพ็กเก็ต IP ขนาดใหญ่ถูกแยกส่วนออกเป็นแฟรกเมนต์ที่มีขนาดเล็กลง แต่ละแฟรกเมนต์จะมีค่า ID เหมือนกันกับแพ็กเก็ตดั้งเดิมของมัน สิ่งนี้ทำให้อุปกรณ์ที่รับข้อมูลสามารถระบุและจัดกลุ่มชิ้นส่วนเข้าด้วยกันเพื่อสร้างแพกเก็ตเดิมขึ้นใหม่ ฟิลด์ ID ในส่วนหัว IP สร้างขึ้นโดยระบบปฏิบัติการที่ส่งและใช้เพื่อระบุแพกเก็ต IP แต่ละรายการ อย่างไรก็ตาม ลักษณะการทำงานเฉพาะและการใช้งานฟิลด์ ID อาจแตกต่างกันไปตามระบบปฏิบัติการต่างๆ ลักษณะของ IPID อาจเปลี่ยนแปลงได้ด้วยการอัปเดตหรือการกำหนดค่าต่างๆ ภายในระบบปฏิบัติการเช่นกัน นอกจากนี้ เวอร์ชันหรือรีลีสของระบบปฏิบัติการอาจมีลักษณะการทำงานที่แตกต่างกัน ดังนั้นค่าความแตกต่างนี้อาจนำมาใช้ไรการแยกแยะระหว่างอุปกรณ์ได้เช่นกัน

จากงาน [Counting NATted Hosts by Observing TCP/IP Field Behaviors] (Mongkolluksamee et al., 2012) แสดงข้อแตกต่างทั่วไปบางประการที่สามารถสังเกตได้จากลักษณะการทำงานของ IPID ในระบบปฏิบัติการต่างๆ

- **Sequential IPID**: ระบบปฏิบัติการบางระบบกำหนดค่า IPID ตามลำดับสำหรับแต่ละแพกเก็ตที่ส่ง ซึ่งหมายความว่าแต่ละแพกเก็ตที่ตามมาซึ่งส่งโดยอุปกรณ์เดียวกันจะมีค่า IPID เพิ่มขึ้น IPID ตามลำดับสามารถให้ความรู้สึกถึงลำดับแพกเก็ตและสามารถช่วยในการประกอบใหม่ได้

- **Incremental IPID**: ระบบปฏิบัติการบางระบบสร้างค่า IPID โดยการเพิ่มค่าคงที่สำหรับแต่ละแพ็กเก็ตที่ส่ง โดยไม่คำนึงถึงแหล่งที่มาเช่นมาจากคนละโปรแกรม วิธีการนี้สามารถคาดการณ์ได้น้อยกว่าเมื่อเทียบกับ IPID ตามลำดับ โดยเฉพาะอย่างยิ่งหากอุปกรณ์หลายเครื่องสร้างแพกเก็ตพร้อมกัน
- **Random IPID:** ระบบปฏิบัติการบางระบบใช้ค่า IPID แบบสุ่มสำหรับแต่ละแพกเก็ตที่ส่ง การสุ่ม IPID สามารถช่วยปรับปรุงความปลอดภัยโดยทำให้ผู้โจมตีคาดเดาหรือติดตามการไหลของแพกเก็ตได้ยากขึ้น อย่างไรก็ตาม การทำเช่นนี้อาจทำให้การประกอบชิ้นส่วนใหม่และการติดตามแพกเก็ตมีความท้าทายมากขึ้น

พฤติกรรมการใช้งานเครือข่ายของ IoT และไม่ใช่ IoT

ด้วยความแตกต่างในลักษณะการทำงานหรือใช้งาน ทำให้อุปกรณ์ IoT และอุปกรณ์ที่ไม่ใช่ IoT นั้นมีพฤติกรรมในการใช้งานเครือข่ายที่แตกต่างเช่น อัตราการส่ง/รับข้อมูลในเครือข่ายทสอดคล้องกับการโต้ตอบของผู้ใช้ จากงาน [A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic] (Apthorpe et al., 2017) ข้อมูลในเครือข่ายที่เกิดขึ้นจากอุปกรณ์ได้รับการกระตุ้นจากภายนอกหรือจากผู้ใช้โดยตรง จะเห็นได้ว่าเมื่ออุปกรณ์ IoT ตรวจพบเหตุการณ์อาทิเช่นมีการขยับตัวของผู้ใช้ในกลุ่มอุปกรณ์ตรวจจับการเคลื่อนไหว อุปกรณ์ก็จะมีการส่งข้อมูลที่สูงขึ้นในทันทีที่มีการตรวจพบเหตุการณ์ หรือเกิดการส่งข้อมูลที่มากขึ้นในอุปกรณ์กลุ่มของ switch เมื่อผู้ใช้มีการสั่งงานเปิดหรือปิด

รูปแบบของโหลดที่เกิดขึ้นจากอุปกรณ์ IoT และที่ไม่ใช่ IoT มีความแตกต่างกัน ซึ่งเกี่ยวข้องโดยตรงจากการออกแบบเพื่อการใช้งานของอุปกรณ์ จากงาน [Characterizing and classifying IoT traffic in smart cities and campuses] (Sivanathan et al., 2017) แสดงให้เห็นว่าอุปกรณ์ IoT นั้นโดยปกติแล้วจะส่งข้อมูลในเครือข่ายน้อยมาก ซึ่งต่างจากอุปกรณ์ที่ไม่ใช้ IoT เช่น computer หรือ mobile phone ซึ่งมักจะมีการใช้งานเครือข่ายมี่สูง เมื่อนำข้อมูลทั้ง IoT และไม่ใช่ IoT มารวมกันจะเห็นได้ว่าปริมาณข้อมูลส่วนใหญ่เกิดจากอุปกรณ์ที่ไม่ใช่ IoT

ปลายทางการสื่อสารของอุปกรณ์ที่เจาะจง อุปกรณ์ IoT นั้นเป็นอุปกรณ์เป็นอุปกรณ์ที่มักระบุปลายทางการสื่อสารไว้ล่วงหน้า เช่นอุปกรณ์พวกนี้มักส่งไปยังเซิร์ฟเวอร์หรือกลุ่มของเซิร์ฟเวอร์ที่เจ้าของผลิตภัณฑ์ได้มีการกำหนดไว้เพื่อให้บริการเฉพาะอุปกรณ์

วิธีดำเนินการ

ขั้นตอนที่ 1 : แหล่งที่มาของชุดข้อมูลสำหรับการวิจัย

ผู้วิจัยนำข้อมูล ตัวอย่างใช้งานภายในระบบเครือข่าย โดยข้อมูลเหล่านั้นจะเป็นฝ่ายนามสกุล pcap ซึ่งเป็นข้อมูลดิบของการใช้งานภายในระบบเครือข่ายโดยละเอียดซึ่งเป็นชุดข้อมูลสาธารณะที่ https://iotanalytics.unsw.edu.au/iottraces.html โดยมีกำหนดอุปกรณ์อยู่ในชุดข้อมูลทั้งหมด 30 อุปกรณ์ โดยอุปกรณ์แต่ละชิ้นนั้นจะถูกระบุอยู่ในไฟล์นามสกุล txt ที่ระบุว่า

อุปกรณ์แต่ละชิ้นใช้งาน mac address อะไรเพื่อระบุตัวตนอุปกรณ์ ซึ่งทั้งหมดจะมีระยะเวลาทั้งหมด 20 วัน โดยแบ่งเก็บเป็น 1 ไฟล์ต่อ 1 วัน

ขั้นตอนที่ 2 : การประมวลผลข้อมูลเพื่อนำไปสร้างแบบจำลองการทำนาย

ในการสร้างชุดข้อมูล เพื่อนำไปเข้าสู่กระบวนการแบบจำลองการทำนายนั้น ข้อมูลที่ได้รับมาจากไฟล์นามสกุล pcap นั้นยังคงเป็นข้อมูลดิบอยู่จึงต้องมีการประมวลผล เพื่อนำข้อมูลที่มีความจำเป็นเท่านั้นเข้าสู่กระบวนการสร้างแบบจำลองการทำนาย โดยการใช้งานภาษา Python โดยการใช้งาน Library ของ Scrapy แต่ก็เพื่อสกัดน้ำข้อมูลที่จำเป็น ออกมาจากไฟล์นามสกุล pcap เป็นข้อมูลที่จำเป็นพร้อมคำนวนสักส่วนค่า IPID ที่ติดลบดังนี้

	Field name	**รายละเอียดของคุณสมบัติ**
1	Number of Flow	เป็นจำนวนครั้งที่ Source IP, Destination IP, Source Port, Destination Port และหมายเลข Protocol ของ packet (Proto) มีค่าแตกต่างกัน
2	Number of Packets	เป็นจำนวน packet ที่เกิดขึ้นทั้งหมดภายในช่วงเวลา 10 นาทีที่ผ่านมา
3	Avg Packet Size	ค่าเฉลี่ยของขนาดของ Packets ในช่วงเวลาทุก 10 นาที
4	Max Packet Size	ค่าที่สูงที่สุดของขนาดของ Packets ในช่วงเวลาทุก 10 นาที
5	Min Packet Size	ค่าที่ต่ำที่สุดของขนาดของ Packets ในช่วงเวลาทุก 10 นาที
6	SD Packet size	ค่าที่มัธยฐานของขนาดของ Packets ในช่วงเวลาทุก 10 นาที
7	IPID_DIFF_negative_ratio	ค่าความแตกต่างระหว่างบรรทัดที่เป็นหมายลบที่ลดลงของ IPID
8	Label	ชนิดของอุปกรณ์

ขั้นตอนที่ 3 : การทำความสะอาดข้อมูล เพื่อนำไปสร้างแบบจำลองการทำนาย

ในการสร้างชุดข้อมูล เพื่อนำไปสร้างแบบจำลองการทำนายนั้นจะใช้งาน ข้อมูลเบื้องต้นจากขั้นตอนที่สองนั้นมาเฉลี่ยเป็นข้อมูล 1 record เนื่องจากปริมาณข้อมูลที่น้อยเกินไปในบางอุปกรณ์ จึงตัดนำข้อมูลที่มีจำนวนต่ำกว่า 2,000 records และอุปกรณ์ที่ไม่ใช่ IoT ออกไปเพื่อความแม่นยำของการทำนายจึงเหลืออุปกรณ์ดังนี้

ชื่ออุปกรณ์	จำนวน record
Smart_Things	2817
Amazon_Echo	2817
Samsung_SmartCam	2817
Dropcam	2817
Belkin_Wemo_switch	2817

	Belkin_wemo_motion_sensor	2817
	Triby_Speaker	2799
	Netatmo_weather_station	2227
	Withings_Smart_Baby_Monitor	2101
	TP_Link_Smart_plug	2100
	Withings_Aura_smart_sleep_sensor	2035
	Light_Bulbs_LiFX_Smart_Bulb	2032
	Insteon_Camera	2030

ขั้นตอนที่ 4 : การสร้างแบบจำลองการทำนาย

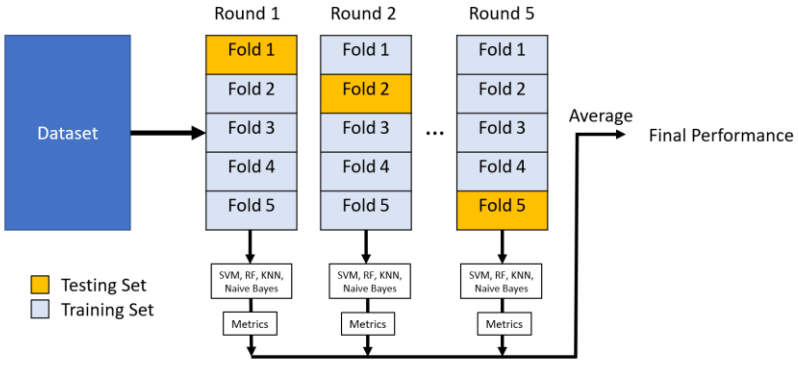
ในการสร้างแบบจำลองการทำนายนั้น ทางผู้วิจัยนั้นได้เลือกใช้แบบจำลองการทำนายทั้งหมด 4 รูปแบบ ดังนี้

1. K-Nearest Neighbors
2. Naive Bayes
3. Random Forest
4. Support Vector Machine

โดยการสร้างแบบจำลองการทำนายนั้นจะไม่มีการปรับแต้งพารามิเตอร์ใดๆ (ใช้งานค่า Default)

ขั้นตอนที่ 5 : การตัดแบ่งข้อมูลออกจากกันทั้ง 5 ส่วนด้วย K-fold Cross Validation

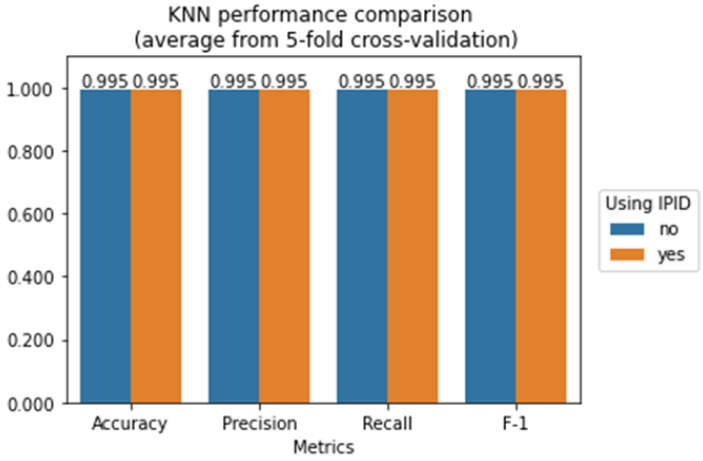
ในการศึกษานี้ ผู้วิจัยได้ตัดแบ่งข้อมูลออกจากกันทั้ง 5 ส่วนเพื่อสร้างความมั่นใจในผลลัพธ์ของแบบจำลองการทำนายหากข้อมูลที่ใช้ในการฝึกฝนและการทำนายนั้นเปลี่ยนไปจะยังคงได้ผลลัพธ์ที่ไม่แตกต่างในการทดลองโดยการแบ่ง 5 ส่วนนั้นจะมีการฝึกฝนและทดลองการทำนายทั้งหมด 5 ครั้งเช่นกัน ดังแสดงในภาพที่ 1



ภาพที่ 1 การทำ Cross Validation แบบ 5 fold

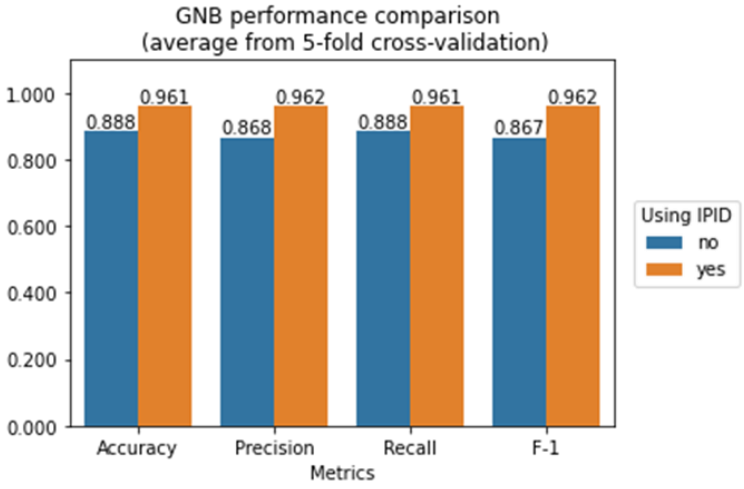
ผลการวิจัยและอภิปรายผลการวิจัย

การทดลองการสร้างแบบจำลองการทำนายนี้ จากการทดลองทั้งหมดทั้ง 4 แบบจำลองการทำนายทั้งหมด 5 ครั้งตามจำนวนของ K-fold Cross Validation และแยกออกเป็น 2 กรณี โดยจะมีการใช้งานค่า IPID และไม่ใช้งานค่า IPID โดยมีผลลัพธ์ดังนี้



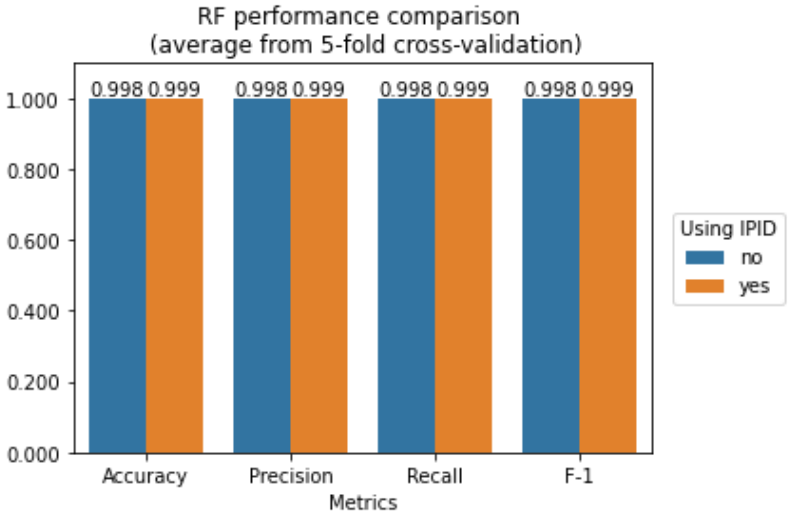
ภาพที่ 2 กราฟแสดงค่าสมรรถนะของแบบจำลองการทำนายของการใช้งานค่า IPID และไม่ใช้งาน IPID ของแบบจำลองการทำนาย K-nearest Neighbors

เมื่อใช้งานด้วยวิธีการ K-nearest Neighbors นั้นพบว่าค่าตัวชี้วัดต่างๆนั้นมีค่าเท่ากันดังแสดงในภาพประกอบที่ 49 การสร้างแบบจำลองการทำนายนี้อาจไม่ได้นำค่า IPID มาเป็นตัวชี้วัดในการจำแนกอุปกรณ์เพิ่มเติม



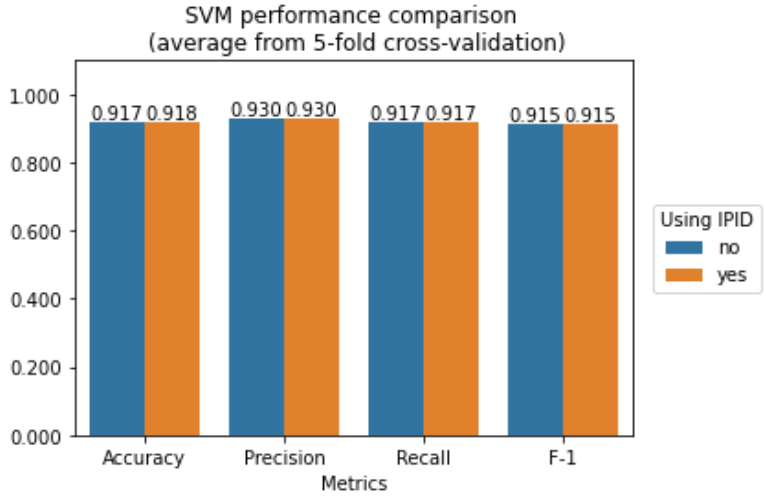
ภาพที่ 3 กราฟแสดงค่าสมรรถนะของแบบจำลองการทำนายของการใช้งานค่า IPID และไม่ใช้งาน IPID ของแบบจำลองการทำนาย Naïve Bayesian

เมื่อใช้งานแบบจำลองการทำนาย Naïve Bayesian แล้วเมื่อนำผลลัพธ์มาเปรียบเทียบดังแสดงในภาพประกอบที่ 50 พบว่าได้รับค่า Accuracy สูงขึ้นเป็น 7.3 เปอร์เซ็นต์ ในส่วนของ Precision นั้นสูงขึ้น 9.4 เปอร์เซ็นต์ ค่า Recall นั้นสูงขึ้นที่ 7.3 เปอร์เซ็นต์ และ F1 นั้นสูงขึ้นที่ 9.5 เปอร์เซ็นต์ แสดงให้เห็นว่าพฤติกรรมของ IPID นั้นสามารถทำให้แบบจำลองการทำนาย Naïve Bayesian นั้นสามารถคาดการณ์อุปกรณ์ได้ง่ายและแม่นยำขึ้น



ภาพที่ 4 กราฟแสดงค่าสมรรถนะของแบบจำลองการทำนายของการใช้งานค่า IPID และไม่ใช้งาน IPID ของแบบจำลองการทำนาย Random Forest

เมื่อใช้นงานแบบจำลองการทำนาย Random Forest แล้วเมื่อนำผลลัพธ์มาเปรียบเทียบดังแสดงในภาพประกอบที่ 51 พบว่าได้รับค่า Accuracy, Precision, Recall และ F1 สูงขึ้นเป็น 0.1 เปอร์เซ็นต์เท่านั้นในทั้งหมด 4 ค่าตัวชี้วัดสมรรถนะของแบบจำลองการทำนาย



ภาพที่ 5 กราฟแสดงค่าสมรรถนะของแบบจำลองการทำนายของการใช้งานค่า IPID และไม่ใช้งาน IPID ของแบบจำลองการทำนาย Support Vector Machine

เมื่อใช้นงานแบบจำลองการทำนาย Support Vector Machine แล้วเมื่อนำผลลัพธ์มาเปรียบเทียบดังแสดงในภาพประกอบที่ 52 พบว่าได้รับค่าความแตกต่างของค่า Accuracy เพียงแค่ 0.1 เปอร์เซ็นต์เพียงเท่านั้น

สรุปผลการวิจัย

งานวิจัยนี้เป็นงานวิจัยการจำแนกอุปกรณ์ IoT โดยการเรียนรู้ของเครื่องเครื่องโดยใช้งานชุดข้อมูลที่เป็นสาธารณะ IoT Traffic Trace จาก UNSW โดยการแปลงข้อมูลทั้งสองครั้ง โดยการเป็นข้อมูลดิบเช่นเดิมแต่ระบบการสร้างแบบจำลองการทำนายนั้นสามารถอ่านข้อมูลได้ในรูปแบบ data frame หรือไฟล์นามสกุล CSV และนำมารวบเป็น 1 record โดยค่าทางสถิติของอุปกรณ์ในทุก 10 นาที นั้นในบางแบบจำลองการทำนายสามารถให้ผลลัพธ์ที่ดีขึ้นหากใช้งาน IPID ร่วมด้วยในการทำนายแต่การเพิ่มคุณสมบัติ IPID นั้นไม่ได้ทำให้ผลลัพธ์ของการสร้างแบบจำลองการทำนายนั่นลดลง

กิตติกรรมประกาศ

การจัดทำาวิจัยได้รับการสนับสนุนจากบัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ ในการนำเสนอผลงานวิจัย ผู้วิจัยจึงขอขอบคุณมา ณ ที่นี้

เอกสารอ้างอิง

Al-Qaseemi, S. A., Almulhim, H. A., Almulhim, M., & Chaudhry, S. R. (2016). IoT architecture challenges and issues: Lack of standardization. *2016 Future Technologies Conference (FTC)*, 731-738.

Aluthge, N. (2017). IoT device fingerprinting with sequence-based features Department of Computer Science. 71-71.

Apthorpe, N., Reisman, D., & Feamster, N. (2017). A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic. http://arxiv.org/abs/1705.06805

Meidan, Y., Bohadana, M., Shabtai, A., Guarnizo, J. D., Ochoa, M., Tippenhauer, N. O., & Elovici, Y. (2017). ProfilIoT: a machine learning approach for IoT device identification based on network traffic analysis. *Proceedings of the ACM Symposium on Applied Computing*, *Part F1280*, 506-509. https://doi.org/10.1145/3019612.3019878

Meidan, Y., Bohadana, M., Shabtai, A., Ochoa, M., Tippenhauer, N. O., Guarnizo, J. D., & Elovici, Y. (2017). Detection of Unauthorized IoT Devices Using Machine Learning Techniques. http://arxiv.org/abs/1709.04647

Mongkolluksamee, S., Fukuda, K., & Pongpaibool, P. (2012). Counting NATted hosts by observing TCP/IP field behaviors. 2012 IEEE International Conference on Communications (ICC),

Sivanathan, A., Gharakheili, H. H., Loi, F., Radford, A., Wijenayake, C., Vishwanath, A., & Sivaraman, V. (2019). Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics. *IEEE Transactions on Mobile Computing*, *18*(8), 1745-1759. https://doi.org/10.1109/tmc.2018.2866249

Sivanathan, A., Sherratt, D., Gharakheili, H. H., Radford, A., Wijenayake, C., Vishwanath, A., & Sivaraman, V. (2017). Characterizing and classifying IoT traffic in smart cities and campuses. *2017 IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2017*, 559-564. https://doi.org/10.1109/INFCOMW.2017.8116438