

การตรวจจับสิ่งผิดปกติบนระบบเครือข่ายมีความสำคัญมากขึ้นในปัจจุบันเนื่องจากการกระทำผิดโดยผู้ไม่ประสงค์ดีซึ่งใช้ช่องทางการสื่อสารที่ตรวจจับได้ยาก เป็นหนึ่งในปัญหาที่พบเจอและสร้างความเสียหายเป็นมูลค่าที่สูง งานวิจัยนี้จึงได้การพัฒนาขั้นตอนวิธีในการตรวจจับการบุกรุกระบบเพื่อให้สามารถป้องกันการกระทำผิดในลักษณะดังกล่าว ด้วยการพัฒนาขั้นตอนวิธีของต้นไม้ตัดสินใจ และ ซัพพอร์ตเวกเตอร์แมทริช เนื่องจากทั้งสองวิธีมีความสามารถตรวจจับสิ่งผิดปกติได้ดีในระดับหนึ่ง แต่ยังมีกรณีการจำแนกผิดพลาดในส่วนที่แตกต่างกัน งานวิจัยนี้จึงได้พัฒนาขั้นตอนวิธีทั้งสองให้ทำงานด้วยกัน เพื่อเป็นการพัฒนาให้ได้ขั้นตอนวิธีใหม่ที่มีความถูกต้องแม่นยำยิ่งขึ้น และผลการทดลองที่ได้สามารถนำไปเป็นแนวทางในการป้องกันระบบที่ต้องการความน่าเชื่อถือที่สูงขึ้นต่อไป

Anomaly detection is becoming more important nowadays since malicious attacks are more difficult to be detected and cause great damages. This research work aims at developing an algorithm for detecting attacks with the use of decision-tree and support vector machine. Since each of these methods is able to detect anomaly well with different level classification errors on different types of anomaly. In this work, these two methods are combined in order to obtain better results which can then be used for improving the system's reliability.