**344-491 สัมมนาวิชาการทางวิทยาการคอมพิวเตอร์**

| | | |
|---|---|---|
| เรื่อง | Framework for Cloud Intrusion Detection System Service | |
| ผู้สัมมนา | นางสาวจันทิมา สุขการ | รหัสนักศึกษา 5710210060 |
| | นางสาวสุพิชชา พัฒนกุล | รหัสนักศึกษา 5710210787 |
| วันที่ | 1 พฤศจิกายน 2560 | เวลา 15.15 – 16.00 น. |
| สถานที่ | ห้อง CS201 ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่ | |

---

**บทคัดย่อ**


อินเทอร์เน็ตในสมัยนี้การใช้ Cloud Computing ทำให้เกิดธุรกรรมทางการเงินออนไลน์เป็นจำนวนมากและมีการแลกเปลี่ยนข้อมูลส่วนบุคคลที่สำคัญผ่านทางอินเทอร์เน็ต ผู้โจมตีสามารถใช้มัลแวร์ประเภทต่างๆในการค้นหาเพราะความอยากรู้หรือการได้มาซึ่งผลประโยชน์จากทางการเงินต่างๆ

งานวิจัยฉบับนี้ผู้วิจัยได้เสนอกรอบการทำงานที่มีประสิทธิภาพซึ่งเรียกว่า LIDF ( Layered Intrusion Detection Framework ) สามารถประยุกต์ใช้กับ cloud computing ใน layer ที่แตกต่างกันเพื่อใช้ในการระบุการจราจรของข้อมูลตามปกติของระบบคลาวด์ โดยใช้การทำเหมืองข้อมูลและนำเครือข่ายประสาทเทียมมาใช้ซึ่งทำให้มีความถูกต้องรวดเร็ว และ LIFD ยังสามารถลดอัตราการจราจรของข้อมูลและทำให้throughputเพิ่มขึ้นได้ โดยไม่มีผลกระทบต่อเป้าหมายหลัก

ผลการทดลองที่ได้จากการใช้ LIDF มาพัฒนาการทำงานในการตรวจจับการบุกรุกในระดับ Layer ต่างๆนี้ เมื่อระบบได้ตรวจจับพฤติกรรมที่ผิดปกติได้แล้ว จะสร้างเป็นรายงานแล้วส่งให้ผู้ดูแลระบบจัดการกับพฤติกรรมเหล่านี้ตามที่กำหนดไว้ และในอนาคตการพัฒนาหรือปรับปรุง LIDF โดยการปรับเปลี่ยนเลเยอร์หรือเพิ่มเลเยอร์มีความเป็นไปได้ จึงคาดว่า LIDF เป็นกรอบการตรวจจับการบุกรุกที่ใช้งานได้ยาวนาน ในขณะเดียวกันการวิจัยในอนาคตนี้จะสามารถแยกการจราจรของข้อมูลที่ผิดปกติและระบุกิจกรรมที่อันตรายได้เพื่อระบุประเภทมัลแวร์ภายในการจราจรของข้อมูลนั้นได้


---

**เอกสารอ้างอิง**


Nouf Saleh Aljurayban, Ahmed Emam. 21-23 March 2015. Framework for cloud intrusion detection system service. *2015 2nd World Symposium on Web Applications and Networking (WSWAN)*, สืบค้นเมื่อวันที่ 22 สิงหาคม 2560, IEEE