การสำรวจ การป้องกันการโจมตีแบบปฏิเสธการให้บริการแบบกระจาย (ดีดีโอเอส) บนสภาพแวดล้อมการประมวลผลแบบคลาวด์

A Survey of Distributed Denial of Service (DDoS) Prevention on Cloud Computing Environment

ณรงค์ฤทธิ์ วังคีรี[1], ก่อเกียรติ แก้วกิ่ง[2], ณัฐกานต์ ชุติมารังสรรค์[3], ศิรปัฐช์ บุญครอง[4]
Narongrit Wangkeeree[1], Korkiat Kaewking[2], Nattakarn Shutimarrungson[3], Sirapat Boonkrong[4]
Received: 20 January 2013 ; Accepted: 30 March 2014

บทคัดย่อ

การประมวลผลแบบคลาวด์ (Cloud Computing) เป็นลักษณะของการทำงานของผู้ใช้งานคอมพิวเตอร์ผ่านอินเทอร์เน็ต ผู้ใช้ไม่จำเป็นต้องทราบถึงกระบวนการของระบบนั้นว่ามีการทำงานอย่างไร และประกอบไปด้วยทรัพยากรอะไรบ้าง ผู้ใช้แค่ระบุความต้องการ ระบบจะจัดสรรทรัพยากรและบริการให้ตรงกับความต้องการผู้ใช้ การประมวลผลแบบคลาวด์ มีการจัดเก็บข้อมูลขนาดใหญ่ เรียกว่า Data Center จึงอาจจะเป็นเป้าหมายของการโจมตีจากผู้ไม่หวังดี การโจมตีประเภทหนึ่งที่มีความร้ายแรงและพบในการประมวลผลแบบคลาวด์ คือการโจมตีแบบ Distributed Denial of Service (DDoS) การโจมตีแบบ DDoS ส่งผลกระทบอย่างรุนแรงกับการประมวลผลแบบคลาวด์ การโจมตีประเภทนี้จะมุ่งใช้ทรัพยากรของการประมวลผลแบบคลาวด์ มากที่สุดจนไม่สามารถให้บริการกับผู้ใช้ได้ โดยเครื่องที่โจมตีมีจำนวนเป็นร้อยถึงพันเครื่องมุ่งโจมตีเครื่องแม่ข่ายเพียงเครื่องเดียว บทความนี้มุ่งเน้นศึกษาหลักการทำงานของการประมวลผลแบบคลาวด์ ปัญหาการโจมตีแบบ DDoS ตลอดถึงวิธีการแก้ปัญหา

คำสำคัญ : การประมวลผลแบบคลาวด์ ปฏิเสธการให้บริการแบบกระจาย (ดีดีโอเอส) การโจมตี

Abstract

Cloud Computing is when the work is processed via the internet on other machines. User you don't need to know how cloud actually works and what it consists of. They only need to specify what they need and the serviced resources will be allocated. Cloud Computing and large data center have become a target of an attack, especially distributed denial of service or DDoS. DDoS aim to use up the resources a cloud so that it cannot service users any more. This paper studies the DDoS attack as well as how to solve it.

Keywords: Cloud Computing, Distributed Denial of Service (DDoS), Attacks

บทนำ

ปัจจุบันนี้ เทคโนโลยีต่างๆ เจริญก้าวหน้าไปอย่างรวดเร็ว โดยเฉพาะเครือข่ายอินเทอร์เน็ต พร้อมกันนั้นก็ยังมีการพัฒนาเทคโนโลยีใหม่ให้เกิดขึ้นอย่างต่อเนื่อง เพื่อตอบสนองความต้องการของผู้สื่อสารข้อมูลบนเครือข่ายอินเทอร์เน็ต ซึ่งทำให้มีการจัดการกับทรัพยากรและบุคลากรเป็นจำนวนมากในการควบคุม และจัดการกับการทำงานเหล่านี้ ดังนั้นจึงทำให้เกิดแนวคิด การประมวลผลแบบคลาวด์หรือ Cloud Computing นี้ขึ้นมา การประมวลผลแบบคลาวด์เป็นลักษณะที่พัฒนาขึ้นต่อมาจากความคิดและบริการของ เวอร์ชวลไลเซชั่น (Virtualization) และเว็บเซอร์วิส (Web service) โดยผู้ใช้งานนั้นไม่จำเป็นต้องมีความรู้ในเชิงเทคนิคสำหรับตัวพื้นฐานการทำงานนั้น[1] การประมวลผลแบบคลาวด์เป็นแนวคิดด้านบริการที่เชื่อมโยงกันโดยคอมพิวเตอร์ต่างๆ ที่ทำงานร่วมกัน ซึ่งอาจตั้งอยู่ในห้องเดียวกันหรือคนละที่ก็ได้ โดยระบบจะทำงานประสานกันแบบรวมศูนย์ คือผู้ใช้ไม่จำเป็น

[1,2,3] *นักศึกษาปริญญาเอก, คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ*
[4] *ผู้ช่วยศาสตราจารย์, คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ*
[1,2,3] *Ph.D. Student, Faculty of Information Technology, King Mongkut's University of Technology North Bangkok*
[4] *Asst.Prof, Faculty of Information Technology, King Mongkut's University of Technology North Bangkok*

ต้องสนใจเลยว่าระบบนั้นมีการทำงานอย่างไร และประกอบไปด้วยทรัพยากรอะไรบ้าง แต่ผู้ใช้แค่ระบุความต้องการ ไปยังซอฟต์แวร์ของการประมวลผลแบบคลาวด์ซอฟต์แวร์จะร้องขอให้ระบบจัดสรรทรัพยากรและบริการให้ตรงกับความต้องการผู้ใช้ โดยระบบสามารถเพิ่มและลดจำนวนของทรัพยากรรวมถึงเสนอบริการให้พอเหมาะกับความต้องการของผู้ใช้ได้ตลอดเวลา และหลังจากนั้นบริการ ก็จะให้ผลลัพธ์แก่ผู้ใช้ ส่วนให้บริการจะไปจัดการกับทรัพยากรอย่างไรนั้นผู้ใช้ไม่จำเป็นต้องสนใจ ดังนั้นจึงสรุปได้ว่า ผู้ใช้นั้นจะมองเห็นเพียงบริการซึ่งทำหน้าที่เสมือนซอฟต์แวร์ที่ทำงานตามความต้องการของผู้ใช้ โดยที่ผู้ใช้ไม่จำเป็นต้องทราบถึงทรัพยากรที่แท้จริงว่ามีอะไรบ้างและถูกจัดการเช่นไร หรือถูกเก็บอยู่ที่ไหน[2] ถึงแม้ว่าการประมวลผลแบบคลาวด์จะมีประโยชน์และใช้บริการที่ค่อนข้างง่าย แต่ก็เป็นช่องทางของการโจรกรรมข้อมูลของผู้ไม่ประสงค์ดี รวมถึงการทำให้การประมวลผลแบบคลาวด์ของผู้ให้บริการไม่สามารถให้บริการได้ การโจมตีแบบ Distributed Denial of Service (DDoS) เป็นการโจมตีประเภทหนึ่งที่ร้ายแรงต่อการประมวลผลแบบคลาวด์ และได้เกิดแนวทางแก้ปัญหา รวมถึงการป้องกัน และงานวิจัยเกิดขึ้นมากมาย

โครงสร้างบทความประกอบด้วย ส่วนที่ 2 ความหมายของการประมวลผลแบบคลาวด์ ส่วนที่ 3 การโจมตีแบบ Distributed Denial of Service (DDoS) ส่วนที่ 4 การป้องกันการโจมตีแบบ DDoS บนการประมวลผลแบบคลาวด์ และส่วนที่ 5 สรุปผล

ความหมายของการประมวลผลแบบคลาวด์

การประมวลผลแบบคลาวด์ (Cloud Computing) นี้เป็นลักษณะของการทำงานของผู้ใช้งานคอมพิวเตอร์ผ่านอินเทอร์เน็ต ที่ให้บริการใดบริการหนึ่งกับผู้ใช้ โดยผู้ให้บริการจะแบ่งปันทรัพยากรให้กับผู้ต้องการใช้งานนั้น[3] จะช่วยลดต้นทุนในการทำธุรกิจโดยไม่จำเป็นต้องมีอุปกรณ์ เปลี่ยนเป็นการเช่าใช้ระบบสารสนเทศจากผู้ให้บริการแทน[6] โดยการให้บริการของการประมวลผลแบบคลาวด์ จะให้บริการในด้านเทคโนโลยีสารสนเทศ แบ่งการให้บริการด้านต่างๆ แบ่งออกเป็นเลเยอร์ ดังนี้ Cloud Platform as a Service (PaaS) เป็นการให้บริการคอมพิวเตอร์เสมือน เพื่อนำมาประมวลผลหรือการทำเป็นเซิร์ฟเวอร์ การให้บริการแบบพร้อมใช้งานทั้งระบบปฏิบัติการ ฐานข้อมูล เว็บ และอีกประเภทคือ Cloud Infrastructure as a Service (IaaS) เป็นการให้บริการที่อยู่ในรูปของพื้นที่ของการจัดเก็บข้อมูล ผู้ใช้สามารถปรับเปลี่ยนขนาดของเนื้อที่ที่ใช้ในการจัดเก็บข้อมูลได้ ซึ่งผู้ให้บริการจะคิดตามขนาดที่ผู้ใช้เรียกใช้งาน และอีกประเภทของ Cloud Software as a Service (SaaS) เป็นการให้บริการโปรแกรมหรือแอพพลิเคชั่น ที่ทำงานอยู่บนการประมวลผลแบบคลาวด์ อาจจะอยู่ในรูปแบบของเว็บแอพพลิเคชั่น โดยโปรแกรมเหล่านี้ใช้บนการประมวลผลแบบคลาวด์ เป็นตัวจัดการ[5]

การโจมตีแบบ Distributed Denial of Service (DDoS)

ปัญหาหลักที่พบในการประมวลผลแบบคลาวด์ คือความปลอดภัยและความเชื่อใจของผู้ใช้บริการ เนื่องจากการที่จะต้องเอาข้อมูลไปฝากไว้กับผู้ให้บริการซึ่งอยู่บนเครือข่ายอินเทอร์เน็ต ซึ่งสามารถเข้าถึงได้ง่าย แต่ก็ทำให้ผู้ใช้บริการมองว่ามีความเสี่ยงมากกว่าใช้ในระบบทั่วไป[7] ในส่วนของการโจมตีแบบ DDoS เพื่อไม่ให้เซิร์ฟเวอร์สามารถให้บริการได้ ถึงแม้ว่าการประมวลผลแบบคลาวด์ จะมี เซิร์ฟเวอร์ ไว้ให้บริการหลายตัวก็ตาม ผู้โจมตีจะมุ่งโจมตีในส่วนของพื้นที่การจัดเก็บข้อมูล ดังนั้นการป้องกันเป็นไปได้ค่อนข้างยากเพราะมีโอกาสเกิดขึ้นได้หลายที่ และหลายๆจุดในเวลาพร้อมๆกัน[6] ซึ่งก็ได้มีงานวิจัยใหม่เพื่อการแก้ไขปัญหาดังกล่าวเพิ่มขึ้นมาเรื่อยๆ[9,10,11,12]

ทั้งนี้ได้สรุปลักษณะการโจมตี และวิธีการแก้ปัญหาได้นำเสนอการโจมตีทั้ง 4 ประเภทที่พบเห็นในปัจจุบัน โดยนำเสนอในตารางที่ 1

การโจมตีแบบ DDoS ผู้โจมตีจะส่งเครื่องมือไปติดตั้งยังเครื่องคอมพิวเตอร์ปลายทาง โดยเครื่องมือจะควบคุมการทำงานของเครื่องคอมพิวเตอร์เหล่านั้น ซึ่งจะเรียกเครื่องคอมพิวเตอร์ที่โดนควบคุมว่า ซอมบี้ (Zombie) ซึ่งเมื่อมีจำนวนพอสมควร ผู้โจมตีก็จะสั่งระดมให้เครื่องซอมบี้ส่งข้อมูลไปยังเหยื่อหรือเป้าหมายที่ต้องการ ซึ่งการโจมตีรูปแบบนี้จะก่อให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่จนผู้อื่นไม่สามารถใช้งานทรัพยากรได้ตามปกติ สำหรับรูปแบบลักษณะการโจมตีสามารถแสดงได้ดังรูปที่ 1 และรูปที่ 2

Table 1 Types of DDoS Attack on Cloud Computing

ลำดับ	ชื่อการโจมตี	ลักษณะการโจมตี	การแก้ปัญหาการโจมตี
1.	SYS Flood [5]	Sending Packet CMP or TCP or UDP packet according to number port such as Port of No.53 (DNS) in the large number of package via target.	Need to filter data before if sending Packet (CMP or TCP or UDP or more than one time.
2.	Smurf Attack [18]	Attacker will send ICMP Echo Request via Broadcast Address in network as medium by doing spoofing of Source IP Address to be IP Address for target attack. The network as medium could send ICMP Echo Replay via IP Address for target at once and could use as bandwidth completely.	Doing filter Packet by configuring of Host and close Ping for ICMP.
3.	HTTP GET Flood [21]	Sending for large requirement via Web Service in order to use a great number of Resources which the Web Service could not be run.	Install and Configure Firewall of user in Web Application for prevent DDoS Attack.
4.	IP spoofing [18]	Spoofing which is the spoofing Packet by sending the great number of IP Address to the target in order to use Resources and the users could not do.	Doing filter Packet for spoofing or a great deal of Ping.

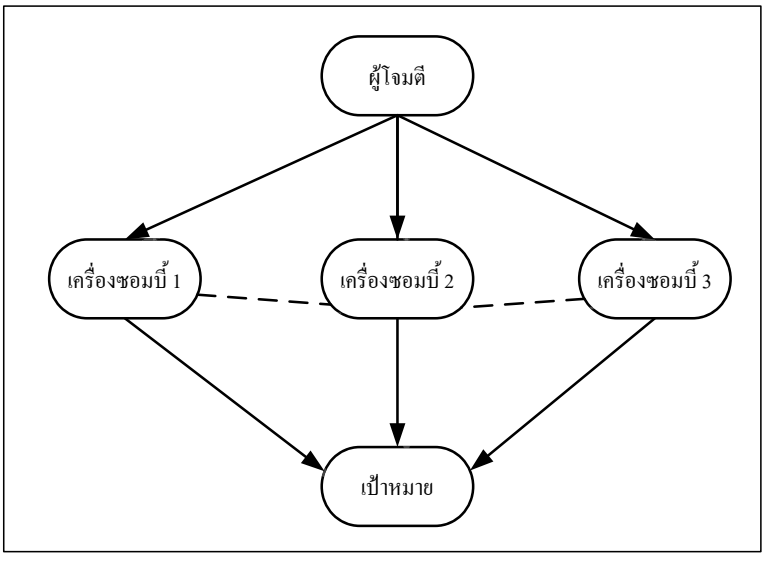

Figure 1 Architecture of DDoS Attack

Figure 1 แสดง Architecture of DDoS Attack โดยมีส่วนประกอบหลักดังนี้

1. เครื่องผู้โจมตี (Attacker) จะเป็นเครื่องแพร่กระจายเครื่องมือในการควบคุมไปยังเครื่องอื่นๆ

2. เครื่องซอมบี้ (Zombie) จะโจมตีพร้อมกันยังเครื่องเป้าหมายเมื่อได้รับคำสั่งหรือเป็นไปตามเงื่อนไข

3. เครื่องเป้าหมายการโจมตี (Target) คือเครื่องเซิร์ฟเวอร์ของการประมวลผลแบบคลาวด์

Figure 2 Architecture of DDoS Attack on Cloud Computing [23]

จาก Figure 2 แสดงรูปแบบการโจมตี DDoS บนการประมวลผลแบบคลาวด์นั้นมีองค์ประกอบคล้ายกับภาพที่ 1 คือหมายเลข 1 เครื่องผู้โจมตี (Attacker) หมายเลข 3 เครื่องซอมบี้ (Zombie) หมายเลข 4 เครื่องเป้าหมาย (Target) และได้เพิ่มในส่วนของหมายเลข 2 คือ เครื่องที่แพร่กระจาย (Botheder) หมายถึง เครื่องที่โดนผู้โจมตี ส่งเครื่องมือเพื่อควบคุมการทำงาน ซึ่งไม่ได้เป็นเครื่องที่โจมตียังเครื่องเป้าหมายโดยตรง แต่เป็นเครื่องที่กระจายเครื่องมือไปควบคุมเครื่องอื่นๆต่อไป

การป้องกันการโจมตีแบบ DDoS บนการประมวลผลแบบคลาวด์

จากการศึกษาค้นคว้าได้มีงานวิจัยเสนอวิธีการป้องกันการโจมตีแบบ DDoS บนการประมวลผลแบบคลาวด์ โดยสามารถแบ่งได้สามวิธีหลักๆ ดังนี้

1. การป้องการโจมตีด้วยการสร้างเครื่องเสมือน

การป้องการโจมตีแบบ DDoS บนการประมวลผลแบบคลาวด์ ด้วยการสร้างเครื่องเสมือน จะวิเคราะห์เกี่ยวกับการโจมตีแบบ Distributed Denial of Service (DDoS) โดยมีการแจ้งเตือน และจัดเก็บข้อมูลลงในฐานข้อมูล SQL ในเครื่องเสมือน และถ้ามีการโจมตีที่ตรงกับข้อมูลที่มีอยู่ใน SQL ก็จะแจ้งเตือน งานวิจัยชิ้นนี้เข้ามาเสริมประสิทธิภาพของการแจ้งเตือนบน IDS เพื่อลดการแจ้งเตือนที่ผิดพลาด โดยงานวิจัยนี้ได้ใช้หลักการ Dempster-Shafer theory (DST) และ Fault-Tree Analysis (FTA) ซึ่ง DST จะนำแพคเกจหรือ Message (m) ที่รับมาทำกระบวนการเพื่อตรวจสอบแพคเกจที่ถูกต้อง ซึ่งจากการวิจัยพบว่าสามารถเพิ่มประสิทธิภาพในแง่ของเวลาตรวจจับและเวลาในการคำนวณ ทำให้ลดการโจมตีแบบ DDoS ได้ในระดับดี[9] และงานวิจัยอีกงานได้ศึกษา การใช้ระบบการตรวจสอบในเครื่องเสมือนที่จำลองขึ้นมาเพื่อใช้ป้องกันการโจมตีก่อนเข้าถึงเครื่องเซิร์ฟเวอร์จริง ซึ่งในงานวิจัยนั้นได้นำเสนอวิธีแก้ปัญหาช่องโหว่ที่ตรวจพบของ โปรโตคอล SOAP ที่ใช้ในการแลกเปลี่ยนข้อมูลระหว่างเว็บเซอร์วิส ด้วยการตรวจสอบ Proxy เพื่อการระบุตัวตนของผู้ขอใช้บริการ และมีการตรวจสอบข้อมูลโดยใช้ XDetector ซึ่งถ้าเป็นผู้ขอใช้บริการจริงก็จะถูกส่งไปยังระบบเซิร์ฟเวอร์ของการประมวลผลแบบคลาวด์[11] และถ้าผู้บุกรุกโจมตีด้วยการสแกนหาพอร์ตของเครื่องเป้าหมาย ด้วยการส่งสัญญาณ SYN หลายๆครั้ง การป้องกันการโจมตี ด้วยการใช้ IDS ในเครื่องเสมือนก็สามารถทำงานได้ดีเช่นกัน แต่งานวิจัยนี้จะสามารถป้องกันการโจมตีแบบ DDoS ได้บางประเภทเท่านั้น[12]

2. การป้องการโจมตีด้วยการตรวจสอบ Packet

การป้องกันการโจมตีแบบ DDoS บนการประมวลผลแบบคลาวด์ ด้วยวิธีการตรวจสอบ Packet โดยจะตรวจจาก IP Address ใน Header ของ Packet โดยจะดูเวลาของการส่งข้อมูล Time-to-live (TTL) และการส่งสัญญาณ SYN ระหว่างไคลแอนต์และเซิร์ฟเวอร์ว่ามีลักษณะผิดปกติหรือไม่ เพื่อหาวิธีการป้องกันต่อไป วิธีนี้เป็นเพียงแค่การตรวจสอบแต่ยังไม่ได้ป้องกันการโจมตีแบบ DDoS[13] และสอดคล้องกับงานวิจัยอีกงานที่ศึกษากลไกแบบ Dual Mechanism ด้วย

การตรวจสอบ Header ของ Packet ว่ามีลักษณะเป็นการโจมตีหรือไม่ โดยการนำหลักการปัญญาประดิษฐ์มาใช้ในระบบ IDS เพื่อการตรวจจับการโจมตีและการแจ้งเตือน และใช้หลักการเอนโทรปี (Entropy) เพื่อลดค่าตัวแปรของ Packet ที่จะตรวจสอบการโจมตี[10] และงานวิจัยอีกชิ้นหนึ่งได้นำเสนอการจัดกลุ่มของข้อมูลโดยใช้หลักการเอนโทรปี ในการจัดเรียงข้อมูล เพื่อลดการโจมตีและการป้องกันทรัพยากรของเครื่องที่เสียไปเนื่องจากการโจมตีแบบ DDoS ด้วยการคำนวณ Packet บนการประมวลผลแบบคลาวด์ ซึ่งพบว่า เมื่อใช้หลักการเอนโทปีแล้วจะทำให้การโจมตีแบบ DDoS บนการประมวลผลแบบคลาวด์ลดลง [14] และส่วนงานวิจัยอีกชิ้นหนึ่งได้ศึกษาการกรอง Packet ด้วยวิธี Confidence-Based Filtering Method (CBF) ซึ่งการกรอง Packet จะแบ่งเป็นสองรูปแบบ คือ แบบที่ไม่มีการโจมตี และแบบที่มีการโจมตี โดยการตรวจสอบ Header ของ TCP และ Header ของ IP พบว่า CBF ที่มีขนาดจัดเก็บข้อมูลขนาดเล็กสามารถกรอง Packet ได้ดีและมีความรวดเร็วในการป้องกันการโจมตีแบบ DDoS บนการประมวลผลแบบคลาวด์[11] สามารถแสดงได้ดังรูปที่ 3

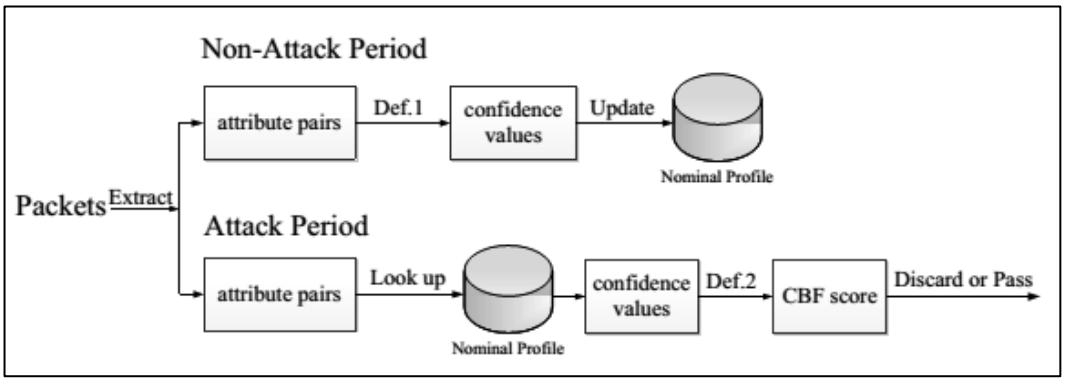

Figure 3 Outline of Confidece-Based Filtering

Figure 3 เป็นการแสดงสถาปัตยกรรมการกรอง Packet ด้วยหลักการของ Confidence-Based Filtering Method (CBF) ซึ่งจะเป็นการกรอง Packet ออกเป็น 2 ส่วน

และอีกงานวิจัยได้ศึกษาการกรอง Packet โดยผู้วิจัยสนใจการทำงานบน Application Layer และได้ทำการทดลองโจมตีสามรูปแบบ เพื่อวัดความแข็งแกร่งของการตรวจจับ ซึ่งสามารถกรอง Packet ที่เป็นการโจมตี ได้ในระดับที่ดี แต่งานวิจัยนี้เพียงวัดประสิทธิภาพของการประมวลผลแบบคลาวด์ ที่มีอยู่แล้วไม่ได้สร้าง เครื่องมือในการป้องกันหรือกรองข้อมูลมาใหม่ และวัดเพียงการโจมตีแค่แบบ FRC เท่านั้น[17] นอกจากนั้นได้มีการศึกษา การป้องการโจมตีแบบ DDoS ด้วยการเรียนรู้การโจมตีหลายรูปแบบ โดยใช้การเรียนรู้แบบโครงข่ายประสาทเทียม พบว่า สามารถตรวจจับหรือป้องกันการโจมตีได้ถึง 91%[19] และอีกงานวิจัยหนึ่งได้ศึกษาการตรวจสอบการโจมตีแบบ Spoof บนเซิร์ฟเวอร์การประมวลผลแบบคลาวด์ซึ่งจะใช้รูปแบบการตรวจสอบการโจมตี ก่อนที่ผู้ใช้จะสามารถเข้าใช้บริการ Data center ได้ ด้วยการตรวจสอบ Packet ที่ส่งไปกับที่รับกลับมาต้องมีความสัมพันธ์กันเสมอ[20]

4.3 การป้องการโจมตีในส่วนของ XML และ HTTP

การป้องการโจมตีแบบ DDoS ในส่วนของ XML และ HTTP ซึ่งเป็นการทำงานของ โปรโตคอล SOAP ที่ช่วยในการสื่อสารของ Web ที่แตกต่างกันให้สามารถสื่อสารกันได้ ข้อความ SOAP จะถูกสร้างโดยใช้ โปรโตคอล HTTP และภาษา XML ซึ่งโจมตีแบบ DDoS รูปแบบหนึ่งจะโจมตีผ่าน HTTP และ XML โดยใช้วิธี CLASSIE และ วิธีการ marking เพื่อทำการตรวจสอบ Packet ซึ่งสามารถหลีกเลี่ยงการโจมตีแบบ Spoofing ได้อย่างมีประสิทธิภาพ ทำให้การโจมตี ลดลงอย่างมาก[21] และสอดคล้องกับอีกงานวิจัยที่ได้ศึกษาการป้องกันการโจมตีเพื่อไม่ให้การประมวลผลแบบคลาวด์สามารถบริการได้ เช่น SaaS, Web Service, Utility Computing และ PaaS เป็นต้น โดยการทำงานของ การประมวลผลแบบคลาวด์จะส่งคำร้องขอในรูป XML แล้วส่งคำร้องนี้โดยผ่าน โปรโตคอล HTTP จากนั้นจะกรองข้อมูลในแบบ tree ซึ่งการทำงานจะเสมือนเป็นการให้บริการแบบ SOA model โดยมีการจัดเก็บข้อมูล Packet ของผู้ใช้บริการ และมีการตรวจสอบ Packet เพื่อกรองข้อมูล ทำให้การโจมตีลดลง[22]

สรุปผล

จากการศึกษาการโจมตีแบบ DDoS บนการประมวลผลแบบคลาวด์ ตลอดจนวิธีในการป้องกันการโจมตี การทำงานของการประมวลผลแบบคลาวด์ ยังขาดความเชื่อมั่นในด้านของความปลอดภัย เพราะทุกอย่างทำงานบนอินเตอร์เน็ต การโจมตีแบบ Distributed Denial of Service (DDoS) เป็นการโจมตีประเภทหนึ่งที่มุ่งเพื่อไม่ให้การประมวลผลแบบคลาวด์สามารถให้บริการกับผู้ใช้ได้ ด้วยการทำให้ทรัพยากรถูกใช้เนื่องจากถูกโจมตี จนเครื่องให้บริการบนการประมวลผลแบบคลาวด์ จึงไม่สามารถให้บริการได้ และมีงานวิจัยที่มุ่งเน้นการป้องกันการโจมตีแบบ DDoS บนการประมวลผลแบบคลาวด์เป็นจำนวนมาก โดยสามารถสรุปเป็นสามวิธีหลัก คือ การป้องกันด้วยการสร้างเครื่องเสมือน (Virtual Machine) เพื่อตรวจสอบข้อมูลก่อนจะเข้าไปยังเครื่องเซิร์ฟเวอร์ของการประมวลผลแบบคลาวด์ วิธีที่สองเป็นการตรวจสอบ Packet ของเครื่องที่ร้องขอใช้บริการว่า Packet ใดเป็น Packet ปกติ และ Packet ใดผิดปกติ และวิธีสุดท้ายคือการป้องกันการโจมตีบน XML และ โปรโตคอล HTTP ในสภาพแวดล้อม SOA โดยจะมีลักษณะคล้ายวิธีการป้องกันการโจมตีแบบการตรวจสอบ Packet ซึ่งทั้งสามวิธีจะสามารถช่วยให้ป้องกันการถูกโจมตีแบบ DDoS ในสภาพแวดลอมการประทวลผลแบบคลาวด์เพิ่มขึ้น

เอกสารอ้างอิง

[1] Lizhe W. and Gregor V. L.,(2008), “Cloud Computing : a Perspective Study,” New Generation Computing Volume28, Number 2, 137-146, DOI: 10.1007/s00354-008-0081-5

[2] Bouzida Y, Cuppens F, Gombault S, (2006), “Detecting and Reacting against Distributed Denial of Service Attacks,” IEEE International Conference on Communication, Volume 5

[3] Sinanc, D., & Sagiroglu, S. (2013, November). A review on cloud security. InProceedings of the 6th International Conference on Security of Information and Networks (pp. 321-325). ACM.

[4] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

[5] Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys (CSUR), 39(1), 3.

[6] Idziorek, J., Tannian, M., & Jacobson, D. (2013). Insecurity of cloud utility models.

[7] Yu, S., Tian, Y., Guo, S., & Wu, D. (2013). Can We Beat DDoS Attacks in Clouds?.

[8] Shi, E., Stoica, I., Andersen, D. G., & Perrig, A. (2006). OverDoSe: A generic DDoS protection service using an overlay network. Computer Science Department, 76.

[9] Lonea, A. M., Popescu, D. E., & Tianfield, H. (2013). Detecting DDoS Attacks in Cloud Computing Environment. International Journal of Computers, Communications & Control, 8(1).

[10] Goyal, U., Bhatti, G., & Mehmi, S. A Dual Mechanism for defeating DDoS Attacks in Cloud Computing Model.

[11] Bakshi, A., & Yogesh, B. (2010, February). Securing cloud from ddos attacks using intrusion detection system in virtual machine. In Communication Software and Networks, 2010. ICCSN’10. Second International Conference on (pp. 260-264). IEEE.

[12] Bakshi, A., & Yogesh, B. (2010, February). Securing cloud from ddos attacks using intrusion detection system in virtual machine. In Communication Software and Networks, 2010. ICCSN’10. Second International Conference on (pp. 260-264). IEEE.

[13] Chouhan, V., & Peddoju, S. K. Packet Monitoring Approach to Prevent DDoS Attack in Cloud Computing. International Journal of Computer Science and Electrical Engineering (IJCSEE) ISSN, (2315-4209).

[14] Jeyanthi, N., Iyengar, N., Kumar, P. C., & Kannammal, A. (2013). An Enhanced Entropy Approach toDetect and Prevent DDoS in Cloud Environment. International Journal of Communication Networks & Information Security, 5(2).

[15] Yang, L., Zhang, T., Song, J., Wang, J., & Chen, P. (2012, May). Defense of DDoS attack for cloud computing. In Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on (Vol. 2, pp. 626-629). IEEE.

[16] Idziorek, J., Tannian, M., & Jacobson, D. (2011, October). Detecting fraudulent use of cloud resources. In Proceedings of the 3rd ACM workshop on Cloud computing security workshop (pp. 61-72). ACM.

[17] Chen, Q., Lin, W., Dou, W., & Yu, S. (2011, December). CBF: A packet filtering method for DDoS attack defense in cloud environment. In Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on (pp. 427-434). IEEE.

[18] Darwish, M., Ouda, A., & Capretz, L. F. (2013, June). Cloud-based DDoS attacks and defenses. In Information Society (i-Society), 2013 International Conference on (pp. 67-71). IEEE.

[19] Joshi, B., Vijayan, A. S., & Joshi, B. K. (2012, January). Securing cloud computing environment against DDoS attacks. In Computer Communication and Informatics (ICCCI), 2012 International Conference on (pp. 1-5). IEEE.

[20] Jeyanthi, N., & Iyengar, N. (2012). Packet Resonance Strategy: A Spoof Attack Detection and Prevention Mechanism in Cloud Computing Environment. International Journal of Communication Networks & Information Security, 4(3).

[21] Anitha, E., & Malliga, S. (2013, February). A packet marking approach to protect cloud environment against DDoS attacks. In Information Communication and Embedded Systems (ICICES), 2013 International Conference on (pp. 367-370). IEEE.

[22] Karnwal, T., Sivakumar, T., & Aghila, G. (2012, March). A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack. In Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on (pp. 1-5). IEEE.

[23] Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys (CSUR), 39(1), 3.