Development and Evaluation of a Hash-Based Intrusion Detection System

Kavita J. Patil and Rohan S. Kulkarni

Kavita J. Patil, Department of Computer Science and Engineering, VIT University, Vellore, India; Rohan S. Kulkarni, Department of Information Technology, University of Pune, Pune, India

ABSTRACT

Security is the main issue in all the sectors but now a days attackers are doing a lot of work to breach this security for their insider trading purpose.They find the number of sources to stole the non public information.In today's life the confidential information is on high risk and become more susceptible for attack.There are many solutions against different types of attack but attacker always try to break the security using new techniques.so here we tried to develop the new technique to resist the attack at much extent.In the proposed work we have implemented Intrusion detection system which is based on hash map.It uses the principle of hashing which stores the object as key-value pair.

Keywords*: Security, Intrusion, Intrusion Detection System.Hash Map,Hashing,Object.*

I. INTRODUCTION

Network Security[3] can be defined as maintaining the confidentiality of private information of individuals ,business environments, conducting transactions,government agencies etc. Most of the security experts are finding the solutions against the attack but day by day attackers are becoming more strong to violate the private data.And it is very important to protect the violations or stealing the data.Attackers may change the original data by gaining unauthorized access to the system or some of the attackers may only read the data to do the future attack.Most of the Intrusion Detection Systems[1] are developed to prevent these attacks And different techniques are already implemented to get the solutions but In the today's environment attackers are becoming more powerfull to break the security and get entry in the system.They violate the confidential data.Some of the techniques of detecting intrusions are as follows[11]:

Firewall: To detect the intrusions, firewall make the use of predefined dynamic rules.It prevents the unwanted entry of illegal traffic from network or the host machine.These firewalls[2] are of different types like Packet Filtering firewall,NAT firewall,Application based firewall,stateful-inspection firewall and hybrid firewall. ,Firewall have the advantages of intrusion detection but have some disadvantages also. Some of the firewalls are unable to find the application layer attacks ,interior attacks[12] ,new threats or some real problems.It does not maintain the consistency of security strategy.

Network IDS: This type of IDS works on network media to capture the packets through cables or wireless devices and compare this packets with the database signatures[7].If packet is matched with stored signature then it states that it an intrusion and then it generate the alert to take the appropriate action.NIDS logs this packet for further detecting the attack of the same type.Example of NIDS :

SNORT: It analyzes the real-time traffic and logs the packets on IP networks.It uses the technique of content matching to identify the probes e.g buffer overflow attack[4].

Firestorm: It includes the preprocessor,decode plugins for protocols[6].It is capable of logging to remote management console**.**

Host IDS:This type of IDS monitors dynamic behavior (packets)as well as the state of a computer system. It identifies which resources accessed by which program .

Hybrid IDS: It is the combination of more than one approach.Example of Hybrid IDS is Prelude which works as both NIDS and reporter server.It captures the network packets and as well as loads the rulsets. Of any NIDS[5].

II. PROPOSED WORK

In this technique Intrusion Detection system detects real time intrusions in the network and provide security with great extent . After detection of attack IDS changes the dynamic rules of firewall automatically.IDS monitors the activities of both user and system and audits the vunerabities.It captures the abnormal activities[9] and maintains the consistency of security strategy.In this paper proposed work includes IDS which is based on hash map which stores the object as key-value pair. It uses the principle of hashing[8].Following figure shows

the mechanism of IDS.Collected information is matched with the hashing technique and then forwarded the message to event generator[10].It generates the alert for admin to take the action or response.

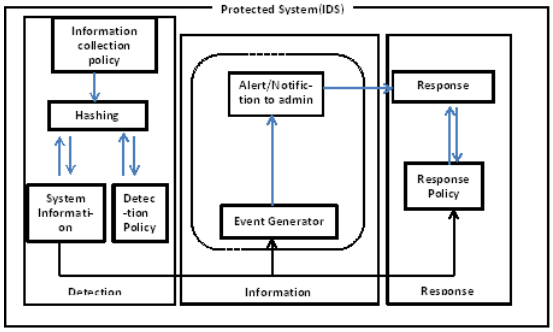

fig -1:IDS Mechanism

III. HASHING TECHNIQUE

Hashing **is a process of assigning a unique code for any object/variable after applying any** algorithm on its properties. A hash function is used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes..

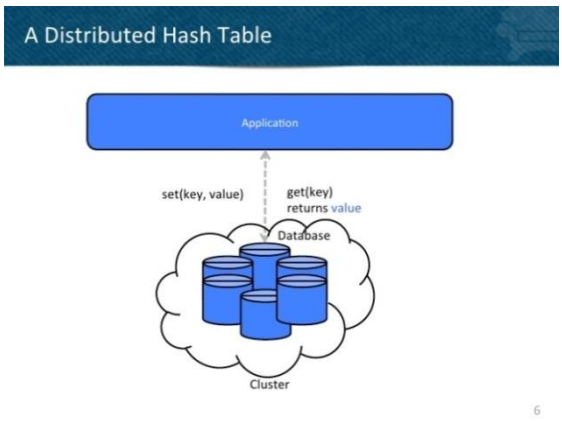

Fig -2:Hashing

ALGORITHM

Consider the following HashMap .

1. class Entry <K,V> implements Map.Entry<K,V>
   final K key;
   V value;
   Entry<K,V> next;
   final int hash; .. }
   Here Entry class has key and value mapping stored as attributes.

2 Calculate hashcode for the key
   Calculate position as
   (hash %(arrayLength-1))
   This adds a new key-value pair

3 (a) put(K key, V value) {
   if (key == null)
   return putForNullKey(value);
   (b) int hash= hash(key.hashCode());
   int i = indexFor(hash, table.length);
   (c) addEntry(hash, key, value, i);
   return null; }
   This creates the HashMap :

4 calculate x.hashCode()
It looks up x in the map.Iterate through the bucket's list by selecting appropriate bucket and pick the entry as e where e.key equals x.
then it returns e.value as given below

(a)
```
List <List<Entry>> buckets;
Object get(Object key) {
 List<List<Entry>bucket=
  buckets.get(key.hashCode()
                    %buckets.size());
```

(b)
```
for (Entry entry : bucket) {
 if (Object.equals(key, entry.key)
 return entry.value; }
  }
```

Table 1: Hashing Methods

Methods	Explanation
public void **put**(K newKey, V data)	-Method allows to put key-value pair in HashMap -If the map already contains a mapping for the key, the old value is replaced. -provide complete functionality how to override equals method. -provide complete functionality how to override hashCode method.
public V **get**(K key)	Method returns value corresponding to key.
public boolean **remove**(K deleteKey)	Method removes key-value pair from HashMapCustom.
public void **display**()	-Method displays all key-value pairs present in HashMapCustom., -insertion order is not guaranteed, for maintaining insertion order refer LinkedHashMapCustom.
private int **hash**(K key)	-Method implements hashing functionality, which helps in finding the appropriate bucket location to store the data. -This is very important method, as performance of HashMapCustom is very much dependent on this method's implementation.

IV. RESULTS

Following figure shows backdoor attack done by the attacker.After receiving alert from event generator admin check the type of attack and take immediate response to prevent the loss of information.

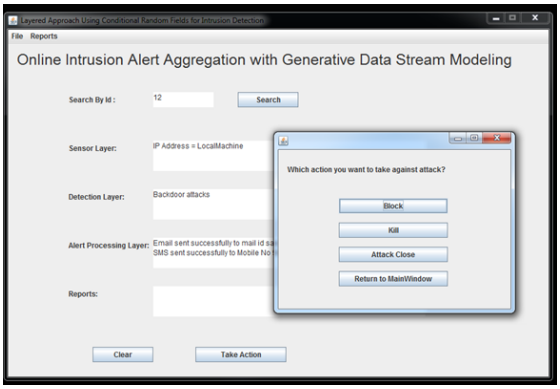

Fig –3:Backdoor Attack

V. CONCLUSION

In the today's IT world everyone wants to keep their confidential data as secure but many of the sources leads to hack the ones confidential information.So taking this under consideration proposed system works to protect the confidentiality, availability and the integrity constraints of the security . This uses the efficient algorithm of hashing technique which works on hashmap.This results in high performance and efficient technology when compared to existing techniques.

REFERENCES

1. *Jadidoleslamy,"weaknesses ,vulnerabilities and elusion strategies against intrusion detection systems",International Journal of Computer Science & Engineering Mohammed Alhanjouri, Ayman M. Al Derawi," A New Method of Query over Encrypted Data in Database using Hash Map", International Journal of Computer Applications (0975 – 8887) Volume 41– No.4, March 2012*
2. *Markus G. Kuhn ,"Eavesdropping attacks on computer displays", Computer Laboratory, University of Cambridge,2006.*
3. *Xiang-Yang Li, "Cryptography and Network Security", CS595*
4. *Akash Mittal, Prof. Ajit Kumar Shrivastava,Dr. Manish Manoria," A Review of DDOS Attack and its Countermeasures in TCP Based Networks", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011*
5. *K.A.Varunkumar, M.Prabakaran,Ajay Kaurav, S.Sibi Chakkaravarthy",Various Databas Attacks and its Prevention Techniques" International Journal of Engineering Trends and Technology (IJETT) – Volume 9 Number 11 - Mar 2014.*
6. *Bhavya Daya ,"Network Security: History, Importance, and Future",University of Florida Department of Electrical a nd Computer Engineering .*
7. *Hector J. Garcia, Jr., Texas A&M University-Kingsville, Dr. Ralph Reilly," TROJAN HORSES: THEY DECEIVE, THEY INVADE, THEY DESTROY", University of Hartford, IACIS 2003.*
8. *Parveen Sadotra,"Hashing Technique - SQL Injection Attack Detection & Prevention", International Journal of Innovative Research in Computer and Communication Engineering(IJIRCCE), Vol. 3, Issue 5, May 2015.*
9. *Jai Puneet Singh," Analysis of SQL Injection Detection Techniques", CIISE, Concordia University.*
10. *Anandarup Sarkar,SvenK¨ohler,Sean Riddle,Bertram Ludasche, Matt Bishop," Insider Attack Identification and Prevention Using a Declarative Approach", 2014 IEEE Security and Privacy Workshops.*
11. *Hossein Survey (IJCSES) Vol.3, No.4, August 2012.*
12. *Jatinder Teji, Rimmy Chuchra, Sonam mahajan, Manpreet Kaur Gill, Manju Dandi, "Detection and Prevention of Passive Attacksin Network Security", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 6, November 2013, ISSN: 2319-5967.*